Guida alla determinazione dei problemi di Lenovo XClarity Administrator

Versione 4.3

Nota

Prima di utilizzare queste informazioni e il prodotto supportato, consultare le informazioni generali e legali nella documentazione online di XClarity Administrator.

Quarta edizione (Aprile 2025)

© Copyright Lenovo 2015, 2025.
NOTA SUI DIRITTI LIMITATI: se i dati o il software sono distribuiti secondo le disposizioni che regolano il contratto "GSA" (General Services Administration), l'uso, la riproduzione o la divulgazione si basa sulle limitazioni previste dal contratto n. GS-35F-05925.

Contenuto

Contenuto i

Riepilogo delle modifiche v

Capitolo 1. Richiesta di supporto e assistenza tecnica 1

Capitolo 2. Visualizzazione di avvisi, eventi e processi 3

Impostazione dei dispositivi in modalità di manutenzione 3
Gestione degli avvisi 4
- Visualizzazione di avvisi attivi 4
- Esclusione di avvisi 8
- Risoluzione di un avviso 9
- Conferma degli avvisi 10

Utilizzo degli eventi 10
- Monitoraggio degli eventi nel log eventi 11
- Monitoraggio degli eventi nel log di controllo 13
- Risoluzione di un evento 14
- Esclusione di eventi 15
- Inoltro di eventi 16

Utilizzo dei processi 50
- Monitoraggio dei processi 50
- Pianificazione dei processi 53
- Aggiunta di una risoluzione e di commenti a un processo 56

Capitolo 3. Utilizzo di assistenza e supporto 57

Ottenere i comunicati da Lenovo 57
Visualizzazione delle informazioni sulla garanzia . . 58
Configurazione dell'invio di notifiche automatiche dei problemi 59
- Configurazione dell'invio di notifiche automatiche dei problemi al supporto Lenovo (Call Home) 60
- Configurazione dell'invio di notifiche automatiche dei problemi alla Funzione Caricamento Lenovo 65
- Configurazione dell'invio di notifiche automatiche dei problemi al fornitore di servizi preferito 69

Modifica della password di ripristino del servizio . . 72
Ispezione dei file di servizio 72
Definizione dei contatti di supporto per dispositivi specifici 73
Raccolta e download dei dati di servizio per un dispositivo 73
Raccolta e download dei file di servizio Lenovo XClarity Administrator 75
Raccolta e download dei file di servizio per un'istanza Lenovo XClarity Administrator che non risponde 77
Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo . . . 78
Segnalazione dei problemi con XClarity Administrator 80
Allegare un file di servizio a un ticket di assistenza aperto 82
Visualizzazione di ticket di assistenza e stato . . . 83
Trasferimento dei dati di servizio al supporto Lenovo 84
Configurazione delle impostazioni log del server di gestione 85
Riabilitazione di Call Home su tutti i dispositivi gestiti 86
Invio di dati periodici a Lenovo 86
- Dati di utilizzo di esempio 88
- Dati hardware di esempio 91

Capitolo 4. Gestione dello spazio su disco 107

Capitolo 5. Problemi di rilevamento e gestione 111

Impossibile rilevare un dispositivo 111
Impossibile gestire un dispositivo 112
Impossibile gestire un dispositivo di storage a causa di un certificato SSL TSL non valido 114
Impossibile gestire uno switch a causa di un certificato SSL TSL non valido 115
Impossibile ripristinare la connettività di uno chassis di Flex System gestito dopo la sostituzione della scheda LED posteriore o dell'assieme del midplane 115
Impossibile ripristinare la connettività di un server gestito dopo la sostituzione della scheda di sistema 116
Incapsulamento non disabilitato dopo l'annullamento della gestione di un server 116
Il nodo di elaborazione non viene visualizzato nell'interfaccia utente dopo la gestione 117
Lo stato di alimentazione del server non è corretto 117

Capitolo 6. Problemi di installazione, rimozione, aggiornamento e migrazione dei dati 119

© Copyright Lenovo 2015, 2025

L'uscita video non funziona quando si installa XClarity Administrator in Red Hat KVM 119
Le modifiche apportate all'adattatore non vengono riconosciute 119
Durante la configurazione iniziale non è possibile avviare la procedura guidata di configurazione iniziale in un browser Web 119
Errore imprevisto della distribuzione di Lenovo XClarity Administrator 120
Aggiornamento di Lenovo XClarity Administratornon riuscito 120

Capitolo 7. Problemi di connettività 121
Impossibile accedere a Lenovo XClarity Administrator 121
Impossibile connettersi a Lenovo XClarity Administrator utilizzando il browser Safari 121
Impossibile eseguire il login 121
Impossibile eseguire il login a Lenovo XClarity Administrator 121
Password per il ripristino locale o un utente supervisore dimenticata 122
Impossibile eseguire il login direttamente al modulo CMM gestito 125
Impossibile eseguire il login direttamente al controller di gestione 125
Impossibile eseguire il login ai server Flex Power System gestiti 125
Perdita improvvisa di connettività a un dispositivo 126

Capitolo 8. Problemi di configurazione di Lenovo XClarity Administrator 127
Problemi di configurazione del server LDAP esterno 127
Non si dispone dell'autorizzazione necessaria a configurare i server 127
Problemi di attivazione di Features on Demand . . 127
Avviso di VMware di mancato supporto del driver VMXNET 3 127

Capitolo 9. Problemi di prestazioni 129
Problemi di prestazioni di Lenovo XClarity Administrator 129
Prestazioni di rete scadenti o lente 129

Capitolo 10. Problemi di sicurezza 131
Il certificato SSL non viene ritenuto attendibile . . . 131
Convalida della certificazione del server non riuscita 131
Vulnerabilità Samba e Apache 132

Capitolo 11. Risoluzione dei problemi di backup e ripristino 135
Il processo di backup sembra bloccarsi durante il riavvio del server di gestione 135
La finestra XClarity Administrator è vuota dopo averla aggiornata durante il backup 135

Capitolo 12. Problemi di monitoraggio e inoltro di eventi 137
Gli eventi non vengono inoltrati 137

Capitolo 13. Problemi relativi alla gestione dei dispositivi 139
Impossibile cancellare in modo sicuro i dati dell'unità sulle unità bloccate 139
Impossibile cancellare in modo sicuro i volumi SDD SATA quando sono collegati a controller RAID Marvell 139
I dati di inventario non vengono aggiornati dopo l'aggiunta o la sostituzione di schede 139

Capitolo 14. Problemi di configurazione dei server 141
Errore durante la creazione di un pattern da un server esistente 141
Errore di attivazione durante la distribuzione di un pattern in un dispositivo 141
Configurazione non valida distribuita in uno switch 142

Capitolo 15. Problemi del repository e dell'aggiornamento firmware 143
Impossibile connettersi al repository Lenovo . . . 143
Dopo l'aggiornamento firmware, Applica/Attiva non mostra la versione firmware aggiornata 143
Impossibile aggiornare il firmware di un dispositivo 143
Blocco dell'aggiornamento firmware di CMM . . . 143
Il firmware viene aggiornato ma non viene eseguito il controllo di conformità 144
Aggiornamenti firmware degli switch Flex System non riusciti 144
Aggiornamento firmware sullo switch Flex System non riuscito con messaggio di errore "Operazione di download del firmware non riuscita". 144
Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore "DCSS_RC_CDT_FAIL" 145
Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di "timeout" 145
Aggiornamento firmware per lo switch Flex non riuscito, con il messaggio di errore "Impossibile scaricare la stessa versione firmware. Scaricare un altro firmware." 145

Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di contatto host non riuscito 146
Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di "file inesistente" 146
Aggiornamento firmware dello switch Flex non riuscito con messaggio di "flashing concluso con errore" 146
Aggiornamento firmware dello switch Ethernet EN6131 40 Gb o dello switch InfiniBand IB6131 non riuscito 146
Aggiornamento firmware di Lenovo EN4091 pass-thru module non riuscito 147
Aggiornamento firmware dello switch Flex System non riuscito con messaggio di errore "Autenticazione chiave host non riuscita" . . . 147
Quando si esegue un aggiornamento, il sistema non riesce a entrare in modalità di manutenzione 147
Il riavvio di un server dal sistema operativo non attiva la modalità di manutenzione 148
Il server che esegue Red Hat Enterprise Linux (RHEL) non si riavvia 148

Capitolo 16. Problemi del repository e di aggiornamento dei driver di dispositivo del sistema operativo . . .149

Impossibile connettersi al sito Web del supporto Lenovo per scaricare gli aggiornamenti dei driver di dispositivo 149
Non è possibile aggiornare i driver di dispositivo su un server 149

Capitolo 17. Problemi di distribuzione del sistema operativo 151

Problemi di report dello stato durante la distribuzione del sistema operativo 151
Impossibile distribuire un sistema operativo 151
Impossibile importare un file nel repository di immagini del sistema operativo 152
Il programma di installazione del sistema operativo non è in grado di trovare l'unità disco su cui si desidera eseguire l'installazione 153
Impossibile avviare il programma di installazione del sistema operativo su un server ThinkServer . . 153
Problemi di distribuzione di VMware ESXi 154
Blocco o riavvio del sistema causato dalla distribuzione VMware 154
Distribuzione VMware non riuscita con errori del disco 154
Il sistema operativo non si riavvia per completare la distribuzione di ESXi su un server ThinkServer 155
Problemi di distribuzione dei sistemi operativi Linux Red Hat e SUSE 155
Distribuzione di Red Hat 6.x non riuscita su server basati su rack con IP statico 156
Distribuzione del sistema operativo non riuscita a causa di driver mancanti 156
Problemi di distribuzione di Microsoft Windows . . 156
La distribuzione del sistema operativo non riesce a causa di partizioni di sistema esistenti su un'unità disco collegata 156

Capitolo 18. Problemi di controllo remoto 159

La sessione di controllo remoto non si avvia 159
La sessione di controllo remoto si blocca dopo il login 159
Non è possibile connettersi a un server 160
Impossibile comunicare con uno switch Flex System dopo l'avvio di una sessione di controllo remoto 160
Non è possibile connettersi a un server in modalità utente singolo 160
Il controllo remoto si connette a un server, ma non è disponibile alcun video 161
Un server non viene visualizzato nell'elenco di aggiunta di una nuova sessione 161
Lo stato del server nella sessione di controllo remoto non corrisponde allo stato in Lenovo XClarity Administrator 161
Un'unità o un'immagine non può essere montata su un server 162
L'opzione supporto di storage non viene visualizzata nell'elenco dei dispositivi di supporto remoto da montare 162
Non è possibile eseguire un'operazione relativa all'alimentazione 162
Il video non è disponibile quando si effettua il collegamento a Server Flex System x280 X6, x480 X6 e x880 X6 162

Capitolo 19. Problemi dell'interfaccia utente 165

Le voci di menu, le icone delle barre degli strumenti e i pulsanti sono disabilitati (evidenziati in grigio) 165
Il browser Web non risponde quando vengono aperte più schede 165
Risposta JSON non riuscita con errore di analisi e altri errori imprevisti 165
L'interfaccia utente non è visualizzata nella lingua preferita 165
Tempi di caricamento lenti o senza risposta, lunga attesa per l'aggiornamento, rendering inappropriato 166
Perdita di dati imprevista 166
Le modifiche apportate alla posizione del dispositivo non vengono applicate nella vista rack 166

© Copyright Lenovo 2015, 2025

Riepilogo delle modifiche

Le versioni successive del software di gestione Lenovo XClarity Administrator supportano nuovi miglioramenti hardware e software, con l'aggiunta di nuove correzioni.

Per informazioni sulle correzioni, fare riferimento al file di cronologia modifiche (*.chg) fornito nel pacchetto di aggiornamento.

In questa versione non sono presenti miglioramenti per la determinazione e la risoluzione dei problemi.

Questa versione supporta i seguenti miglioramenti per la determinazione e la risoluzione dei problemi.

Per informazioni sulle modifiche nelle release precedenti, vedere Novità nella documentazione online di XClarity Administrator.

Funzione	Descrizione
Assistenza e supporto	Il supporto per l'API tcpdump è stato aggiunto per aiutare il supporto Lenovo durante le interazioni con i clienti.

© Copyright Lenovo 2015, 2025

Capitolo 1. Richiesta di supporto e assistenza tecnica

Se è necessario ricevere informazioni sulla guida, supporto o assistenza tecnica per Lenovo XClarity Administrator, è possibile accedere ai vari servizi Lenovo predisposti a questo scopo.

Prima di iniziare

Per informazioni generali su numeri di contatto, risorse e suggerimenti che consentono di ottenere il migliore supporto possibile, dove e quando necessario, vedere Piano di supporto Lenovo - Pagina Web del software.

Procedura

- Porre domande e individuare le risposte facendo clic sul menu azioni utente (

) sulla barra del titolo di XClarity Administrator, quindi su **Visita forum** o accedendo direttamente al Sito Web del forum della community dedicata a Lenovo XClarity.
- Inviare idee e fornire feedback su XClarity Administrator facendo clic sul menu azioni utente (

) sulla barra del titolo di XClarity Administrator, quindi su **Invia idee** o accedendo direttamente a Sito Web di Lenovo XClarity Ideation.
- Controllare il log eventi e attenersi alle azioni suggerite per risolvere tutti i codici di evento (vedere Utilizzo degli eventi).
- Trovare soluzioni ai problemi con sintomi identificabili e attenersi alle azioni suggerite per risolverli. Per ottenere le procedure aggiornate di risoluzione dei problemi, vedere Risoluzione dei problemi nella documentazione online di XClarity Administrator.
- Consultare Sito Web del supporto per i data center Lenovo per i più recenti suggerimenti e le tecniche da utilizzare per risolvere i problemi che si potrebbero riscontrare con XClarity Administrator. Questi *suggerimenti tecnici* descrivono le procedure per la risoluzione di problemi relativi all'utilizzo di XClarity Administrator.

  Per conoscere i suggerimenti tecnici disponibili per il server:

  1. Consultare Sito Web del supporto per i data center Lenovo.
  2. Immettere "XClarity Administrator" nel campo **Cerca**.
  3. Fare clic su **Visualizza tutto** nella sezione **Articoli principali** per visualizzare tutti i suggerimenti o immettere le parole chiave nel campo **Cerca** per trovare un suggerimento specifico.

     Suggerimento: è possibile ordinare l'elenco di suggerimenti per **Pertinenza**, **Popolarità** o **Più recenti**.
- In presenza di un problema hardware o del controller di gestione della scheda di base con un dispositivo gestito, consultare la documentazione fornita con il dispositivo per ottenere informazioni sui problemi e le azioni suggerite.
  - Per le appliance ThinkAgile, vedere Documentazione online di ThinkAgile.
  - Per i prodotti ThinkSystem, inclusi server e dispositivi di rete, vedere Documentazione online di ThinkSystem.
  - Per i prodotti Converged, System x e RackSwitch, inclusi server e switch TOR (Top-of-Rack), vedere la Documentazione online di System x.
  - Per i prodotti NeXtScale, vedere la Documentazione online di NeXtScale.
  - Per i prodotti Flex System, inclusi chassis, switch, dispositivi di storage e nodi di elaborazione, vedere la Documentazione online di Lenovo Flex System.

© Copyright Lenovo 2015, 2025

- Se il problema riguarda il server di gestione XClarity Administrator, è possibile inviare manualmente un ticket di assistenza (vedere Segnalazione dei problemi con XClarity Administrator).
- Se il problema persiste e l'utente è un cliente autorizzato con un contratto di supporto in linea, accordi di manutenzione e/o garanzia, inviare una richiesta di servizio online.

  Nota: Lenovo XClarity Pro include il servizio di assistenza e supporto e la licenza di abilitazione di tutte le funzioni per XClarity Administrator. Per informazioni sull'acquisto di Lenovo XClarity Pro, contattare un rappresentante Lenovo o un business partner autorizzato.

  L'invio di una richiesta di servizio avvia il processo atto a determinare una risoluzione del problema rendendo le informazioni pertinenti disponibili per il Supporto Lenovo in modo rapido ed efficiente. I tecnici dell'assistenza Lenovo potranno iniziare a gestire la risoluzione in seguito al completamento e all'invio di una richiesta.

  Nota: Se Call Home è configurato e abilitato, XClarity Administrator apre automaticamente un ticket di assistenza e trasferisce i file di servizio al Centro assistenza clienti Lenovo quando si verifica un evento che richiede assistenza per la risoluzione del problema. Per informazioni sull'abilitazione di Call Home, vedere Configurazione dell'invio di notifiche automatiche dei problemi al supporto Lenovo (Call Home).

  Se la funzione Call Home non è abilitata, è possibile inviare manualmente una richiesta di servizio e inviare i file di servizio (vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo).

  Nota: IBM è il fornitore di servizi preferito di Lenovo per XClarity Administrator. Le richieste di servizio per alcuni dispositivi vengono inoltrate a IBM per l'assistenza.
- Tramite i servizi di supporto tecnico Lenovo, è possibile ottenere assistenza tecnica, a pagamento, per l'utilizzo, la configurazione e problemi di software con i prodotti Lenovo.

  Per individuare i numeri di telefono del supporto locale e il numero verde, vedere Sito Web dei numeri di telefono del supporto. È possibile comporre il numero per la propria area geografica oppure fare clic su **Contatti** nella pagina Web per ottenere assistenza.

  Per problemi di gravità 1, il supporto è disponibile 24 ore su 24, 7 giorni su 7. Per tutti gli altri problemi, le ore di funzionamento e le lingue sono elencate nella pagina Web della propria area geografica.

  Per contattare il supporto dei prodotti per la Cina, vedere Lenovo Services - Sito Web per la Cina. È inoltre possibile chiamare il numero 400-106-8888 per ottenere supporto per il prodotto. Il supporto telefonico è disponibile dal lunedì al venerdì, dalle 9.00 alle 18.00.

Capitolo 2. Visualizzazione di avvisi, eventi e processi

Lenovo XClarity Administrator fornisce diversi metodi che è possibile utilizzare per monitorare lo stato dei dispositivi gestiti.

- L'elenco di avvisi fornisce una vista in tempo reale dei problemi identificati con XClarity Administrator o qualsiasi dispositivo gestito.
- Il log di controllo e il log eventi forniscono una vista cronologica degli interventi dell'utente e delle azioni di eventi identificati da XClarity Administrator.
- Il log dei processi fornisce un elenco delle attività in esecuzione più lunghe eseguite con uno o più dispositivi gestiti.

Impostazione dei dispositivi in modalità di manutenzione

Quando un dispositivo è in modalità di manutenzione, Lenovo XClarity Administrator esclude tutti gli eventi e gli avvisi per tale dispositivo da tutte le pagine in cui sono visualizzati gli eventi e gli avvisi. Gli avvisi esclusi vengono comunque registrati ma nascosti alla vista.

Informazioni su questa attività

Sono esclusi soltanto gli eventi e gli avvisi generati per un dispositivo mentre questo è in modalità di manutenzione. Gli eventi e gli avvisi prima che il dispositivo venisse messo in modalità di manutenzione vengono invece visualizzati.

La riattivazione di un dispositivo gestito precedentemente impostato in modalità di manutenzione potrebbe rendere obsoleto l'inventario per tale dispositivo. In caso di anomalie, aggiornare manualmente l'inventario dalla pagina del dispositivo selezionando il dispositivo stesso e facendo clic su **Tutte le azioni → Inventario → Aggiorna inventario**.

Procedura

Completare una delle seguenti operazioni per impostare i dispositivi in modalità di manutenzione.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.

Passo 3. Selezionare uno o più dispositivi da impostare in modalità di manutenzione.

Passo 4. Fare clic su **Azioni → Manutenzione** per visualizzare la finestra di dialogo Modalità di manutenzione.

Passo 5. Selezionare la data e l'ora per la riattivazione del dispositivo.

Selezionare **Indefinita** se non si desidera riattivare il dispositivo.

Passo 6. Fare clic su **Conferma**. La colonna di manutenzione nella tabella viene modificata in Sì per tale dispositivo.

Al termine

Una volta completata la manutenzione del dispositivo, è possibile riattivare il dispositivo selezionandolo e facendo clic su **Azioni → Manutenzione**, quindi facendo clic su **Disattiva manutenzione** nella finestra di

© Copyright Lenovo 2015, 2025

dialogo. Se il dispositivo non viene manualmente riattivato (rimesso in funzione), viene automaticamente impostato in modalità di servizio allo scadere del tempo specificato.

Gestione degli avvisi

Gli *avvisi* sono condizioni hardware o di gestione che richiedono l'analisi e l'intervento dell'utente. Lenovo XClarity Administrator esegue il polling dei dispositivi gestiti in modo asincrono e visualizza avvisi ricevuti da tali dispositivi.

Informazioni su questa attività

Ulteriori informazioni: XClarity Administrator: monitoraggio

Di norma, quando si riceve un avviso, un evento corrispondente viene archiviato nel log eventi. È possibile che a un avviso non corrisponda alcun evento nel log eventi (nonostante il wrapping del log). Ad esempio, gli eventi che si verificano prima di gestire uno chassis non vengono visualizzati nel log eventi. Tuttavia, gli avvisi per lo chassis vengono visualizzati nel log avvisi poiché Lenovo XClarity Administrator esegue il polling di CMM dopo che lo chassis è stato gestito.

Visualizzazione di avvisi attivi

È possibile visualizzare l'elenco di tutti gli avvisi hardware e di gestione attivi.

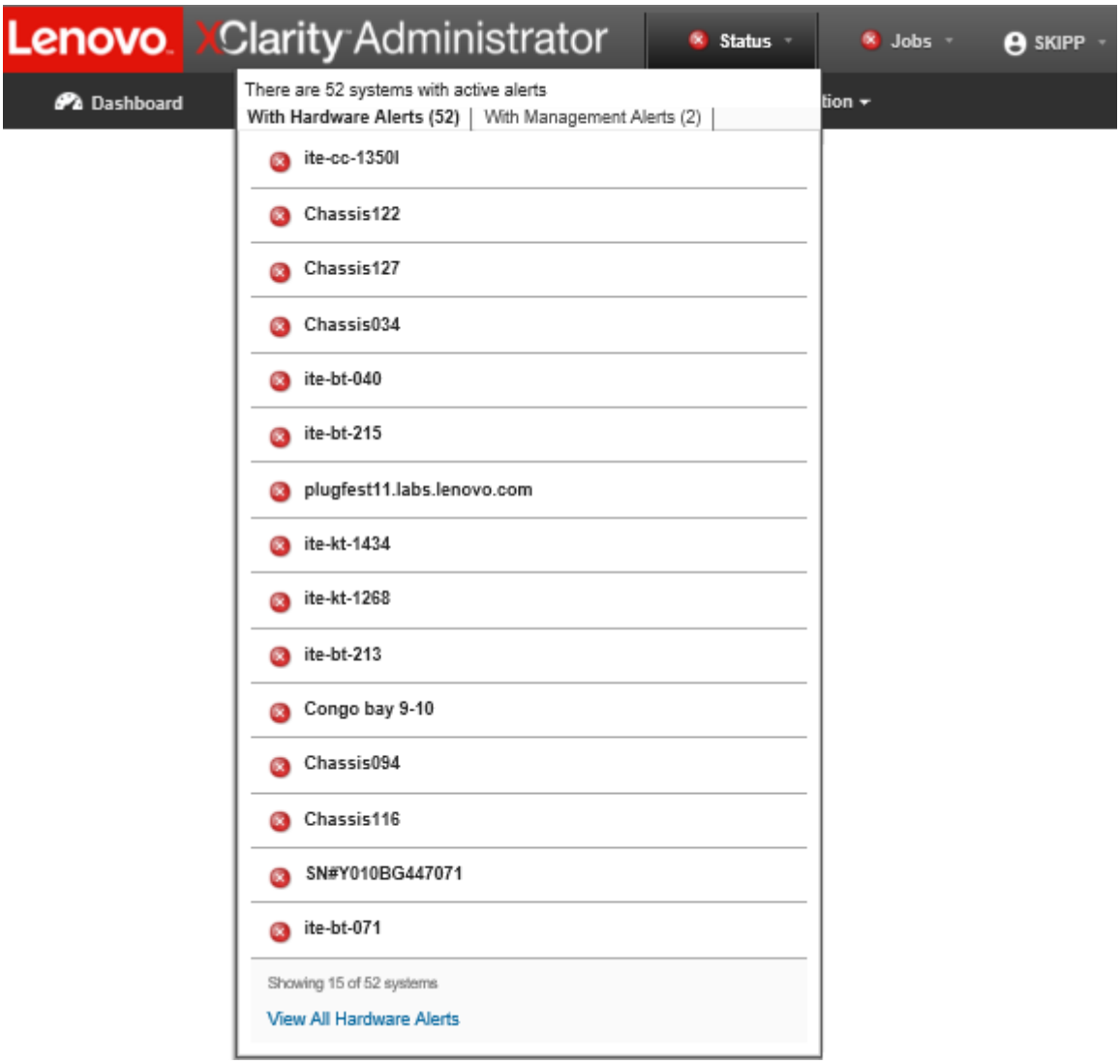
Informazioni su questa attività

Nota: gli avvisi per i dispositivi Lenovo Storage vengono visualizzati solo in inglese, anche se le impostazioni locali di Lenovo XClarity Administrator sono configurate su un'altra lingua. Se necessario, utilizzare un sistema di traduzione esterno per tradurre i messaggi manualmente.

Procedura

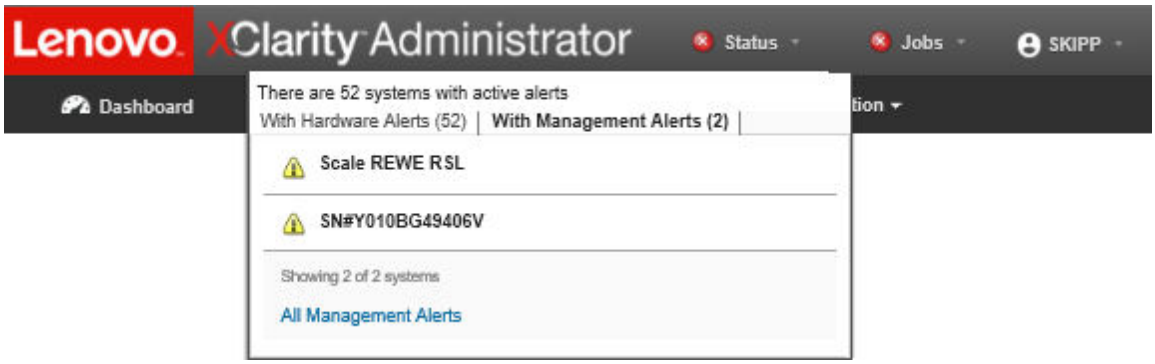
Per visualizzare gli avvisi attivi, completare una di queste procedure.

- Per visualizzare solo gli avvisi per i dispositivi gestiti (noti come *avvisi hardware):*
  1. Nella barra del titolo di XClarity Administrator fare clic sull'elenco a discesa **Stato** per visualizzare un riepilogo degli avvisi hardware e di gestione.
  2. Fare clic sulla scheda **Con avvisi hardware** per visualizzare un riepilogo degli avvisi per ogni dispositivo gestito.



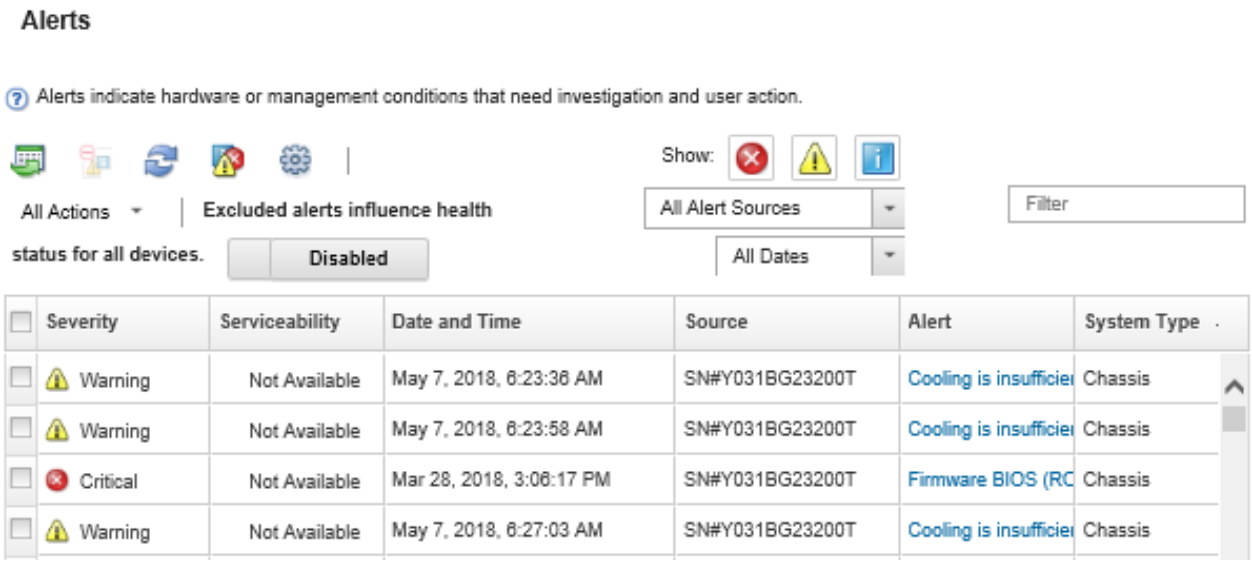
3. Passare il cursore su un dispositivo elencato in tale scheda per visualizzare l'elenco dei relativi avvisi.
4. Fare clic sul collegamento **Tutti gli avvisi hardware** per visualizzare la pagina Avvisi con un elenco filtrato di tutti gli avvisi hardware.

- Per visualizzare solo gli avvisi di XClarity Administrator (noti come *avvisi di gestione*):
  1. Nella barra del titolo di XClarity Administrator fare clic sull'elenco a discesa **Stato** per visualizzare un riepilogo degli avvisi hardware e di gestione.
  2. Fare clic sulla scheda **Con avvisi di gestione** per visualizzare un riepilogo di tutti i CMM e degli avvisi di XClarity Administrator.



3. Passare il cursore su un dispositivo elencato in tale scheda per visualizzare l'elenco dei relativi avvisi.
4. Fare clic sul collegamento **Tutti gli avvisi di gestione** per visualizzare la pagina Avvisi con un elenco filtrato di tutti gli avvisi del CMM e di XClarity Administrator.

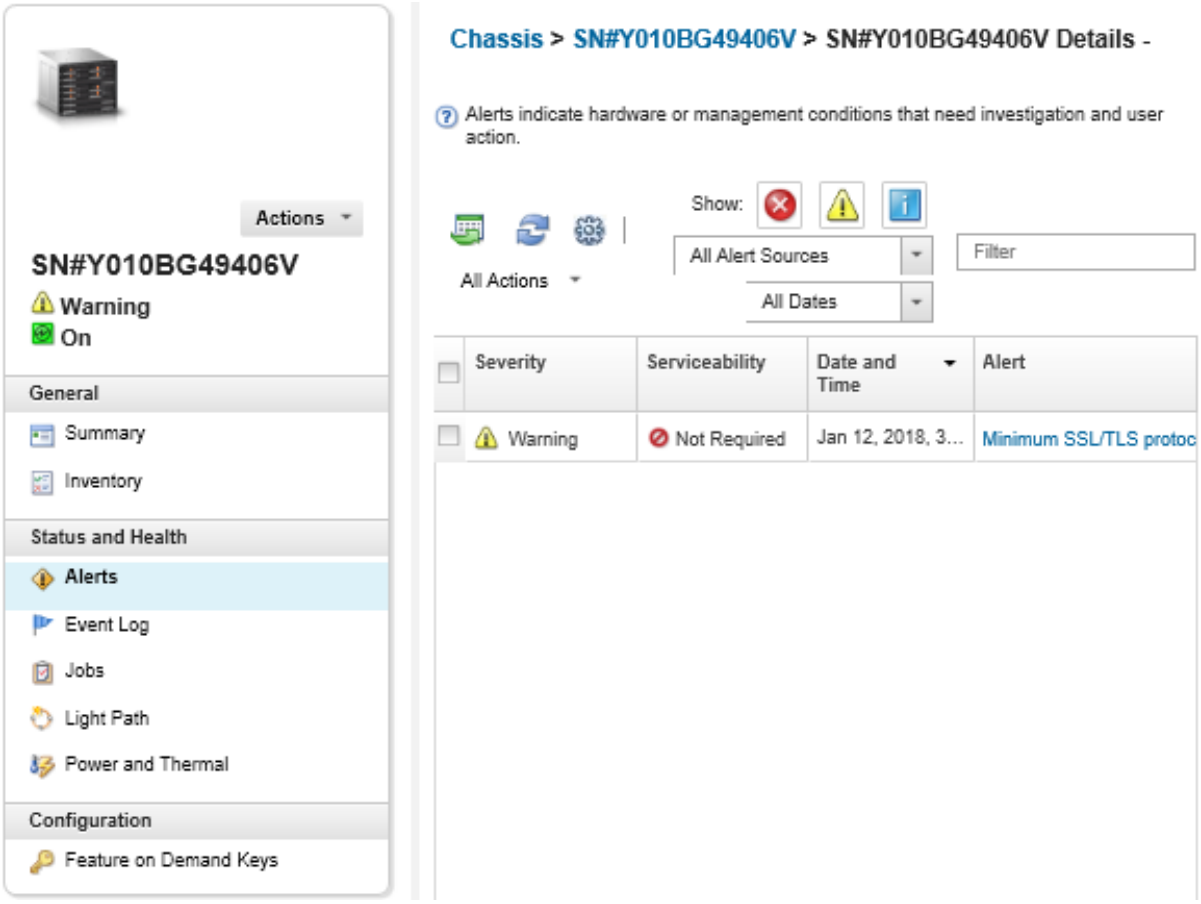
- Per visualizzare tutti gli avvisi in XClarity Administrator, fare clic su **Monitoraggio → Avvisi** nella barra dei menu di XClarity Administrator. Verrà visualizzata la pagina Avvisi con l'elenco di tutti gli avvisi attivi.



- Per visualizzare gli avvisi per uno specifico dispositivo:
  1. Nella barra dei menu di XClarity Administrator fare clic su **Hardware** e selezionare un tipo di dispositivo. Verrà visualizzata una pagina contenente una vista tabulare di tutti i dispositivi gestiti di tale tipo. Ad esempio, fare clic su **Hardware → Server** per visualizzare la pagina Server.
  2. Fare clic su uno specifico dispositivo per visualizzare la pagina Riepilogo per il dispositivo.
  3. In Stato e integrità fare clic su **Avvisi** per visualizzare l'elenco di tutti gli avvisi associati a tale dispositivo.

     Nota: nella colonna Intervento richiesto è possibile che venga visualizzato il messaggio "Non disponibile" se:

     – L'avviso sul dispositivo è stato visualizzato prima che XClarity Administrator iniziasse a gestirlo.
     – Il wrapping del log eventi ha fatto sì che l'evento associato a tale avviso non sia più nel log eventi.



Risultati

Dalla pagina Avvisi è possibile completare le seguenti azioni:

- Aggiornare l'elenco degli avvisi facendo clic sull'icona **Aggiorna** ( ).

  Suggerimento: Se vengono rilevati nuovi avvisi, il log avvisi si aggiorna automaticamente ogni 30 secondi.
- Visualizzare informazioni su un avviso specifico (inclusa una descrizione e l'intervento dell'utente) e sul dispositivo da cui ha avuto origine l'avviso (come l'UUID) facendo clic sul collegamento nella colonna **Avviso**. Verrà visualizzata una finestra di dialogo con dettagli e informazioni sulle proprietà degli avvisi.

  Nota: Se la descrizione e le azioni di ripristino di un avviso non sono visualizzate nella scheda **Dettagli**, andare al Documentazione online di Lenovo Flex System e cercare l'ID dell'avviso (ad esempio, `FQXHMSE0004G`). Nel sito Web sono sempre disponibili le informazioni più aggiornate.
- Per impostazione predefinita, gli avvisi esclusi non incidono sullo stato dell'integrità dei dispositivi gestiti. È possibile consentire agli avvisi esclusi di incidere sullo stato dell'integrità dei dispositivi gestiti dalla pagina Avvisi, facendo clic sull'interruttore per abilitare **Gli eventi esclusi incidono sullo stato di integrità di tutti i dispositivi**.
- È possibile impostare le preferenze delle soglie per la generazione di un avviso e di un evento quando un determinato valore, come la durata di un'unità SSD di un server ThinkSystem o ThinkServer, supera un livello di avvertenza o critico (vedere Impostazione delle preferenze delle soglie per la generazione di avvisi ed eventi nella documentazione online di XClarity Administrator).
- Esportare il log avvisi facendo clic sull'icona **Esporta come CSV** ( ).

Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.

- Escludere avvisi specifici da tutte le pagine in cui sono visualizzati gli avvisi (vedere Esclusione di avvisi).
- Limitare l'elenco di avvisi visualizzati nella pagina corrente:
  - Mostrare o nascondere gli avvisi di una gravità specifica facendo clic sulle seguenti icone:
    - Icona **Avvisi critici** ( )
    - Icona **Avvisi di avvertenza** ( )
    - Icona **Avvisi informativi** ( )
  - Mostrare solo avvisi di origini specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le origini avvisi
    - Eventi hardware
    - Eventi di gestione
    - Eventi centro di assistenza
    - Eventi manutenibili cliente
    - Eventi non manutenibili
  - Mostrare solo avvisi con data e ora specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le date
    - Due ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
  - Elencare solo gli avvisi che contengono testo specifico immesso nel campo **Filtro**.
  - Ordinare gli avvisi per colonna facendo clic su un'intestazione di colonna.

Esclusione di avvisi

Avvisi specifici ritenuti inutili dall'utente possono essere esclusi da tutte le pagine in cui vengono visualizzati. Gli avvisi esclusi rimangono continuano a essere presenti nel log ma non vengono visualizzati in nessuna delle pagine dedicate agli avvisi, incluse le visualizzazioni del log e lo stato del dispositivo.

Informazioni su questa attività

Gli avvisi esclusi vengono nascosti a tutti gli utenti e non solo all'utente che imposta la configurazione.

È possibile impostare i dispositivi in modalità di manutenzione, in modo da escludere tutti gli eventi e gli avvisi relativi a questi dispositivi (vedere Impostazione dei dispositivi in modalità di manutenzione).

Restrizione: solo gli utenti con privilegi di amministratore possono escludere o ripristinare gli avvisi.

Importante: se si escludono gli avvisi di stato, lo stato del dispositivo nel riepilogo dei dispositivi e nelle pagine dei dettagli rimarrà inalterato.

Procedura

Per escludere avvisi dal log avvisi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi**. Verrà visualizzata la pagina Avvisi.

Passo 2. Selezionare gli avvisi da escludere e fare clic sull'icona **Escludi avvisi** ( ). Verrà visualizzata la finestra di dialogo Escludi avvisi.

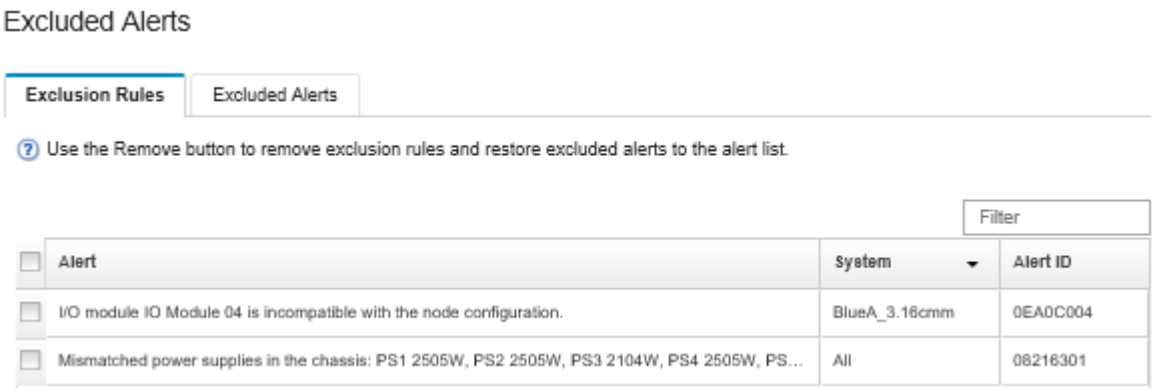
Passo 3. Selezionare una delle seguenti opzioni:

- **Escludi avvisi selezionati da tutti i sistemi**. Esclude gli avvisi selezionati da tutti i dispositivi gestiti.
- **Escludi avvisi solo dai sistemi nell'ambito dell'istanza selezionata**. Esclude gli avvisi selezionati dai dispositivi gestiti a cui si applicano.

Passo 4. Fare clic su **Salva**.

Al termine

Quando si escludono avvisi, Lenovo XClarity Administrator crea regole di esclusione basate sulle informazioni fornite. È possibile visualizzare un elenco di regole di esclusione e di avvisi esclusi dalla pagina Avvisi facendo clic sull'icona **Mostra avvisi esclusi/confermati** ( ). Nella finestra di dialogo Avvisi esclusi/confermati fare clic sulla scheda **Regole di esclusione** per visualizzare l'elenco delle regole di esclusione oppure fare clic sulla scheda **Avvisi esclusi** per visualizzare l'elenco degli avvisi esclusi.



Per impostazione predefinita, gli avvisi esclusi non incidono sullo stato dell'integrità dei dispositivi gestiti. È possibile consentire agli avvisi esclusi di incidere sullo stato dell'integrità dei dispositivi gestiti dalla pagina Avvisi, facendo clic sull'interruttore per abilitare **Mostra avvisi esclusi/confermati**.

È possibile ripristinare gli avvisi esclusi nel log avvisi rimuovendo la regola di esclusione appropriata. Per rimuovere una regola di esclusione, fare clic sull'icona **Mostra eventi esclusi** ( ) per visualizzare la relativa finestra di dialogo, selezionare le regole di esclusione o l'avviso escluso da ripristinare e fare clic su **Rimuovi**.

Risoluzione di un avviso

Lenovo XClarity Administrator fornisce informazioni sulle azioni appropriate da eseguire per risolvere un avviso.

ProceduraPer risolvere un avviso, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi** per visualizzare la pagina Avvisi.

Passo 2. Individuare l'avviso nel log avvisi.

Passo 3. Fare clic sul collegamento nella colonna **Avviso** per visualizzare informazioni sull'avviso (inclusa una descrizione e le azioni di ripristino) e le proprietà del dispositivo da cui l'avviso ha avuto origine (come l'UUID).

Passo 4. Per risolvere l'avviso, attenersi alle azioni di ripristino elencate nella scheda **Dettagli**. L'esempio seguente mostra le azioni di ripristino di un evento.

Modificare l'impostazione del criterio di sicurezza sullo chassis gestito di riferimento affinché corrisponda al criterio di sicurezza corrente sul server di gestione.

Per modificare il criterio di sicurezza nello chassis, aprire una sessione dell'interfaccia della riga di comando su Chassis Management Module (CMM) ed eseguire uno dei seguenti comandi:

- Per modificare il livello di criteri di sicurezza in `Secure`:
  ```
  security -p secure -T mm[p]
  ```
- Per modificare il livello di criteri di sicurezza in `Legacy`:
  ```
  security -p legacy -T mm[p]
  ```

Nota: Se la descrizione e le azioni di ripristino di un avviso non sono visualizzate nella scheda **Dettagli**, andare al Documentazione online di Lenovo Flex System e cercare l'ID dell'avviso (ad esempio, `FQXHMSE0004G`). Nel sito Web sono sempre disponibili le informazioni più aggiornate.

Se, dopo essersi attenuti alla procedura consigliata, il problema persiste, contattare il Supporto Lenovo.

Conferma degli avvisi

Quando viene confermato un avviso attivo, l'avviso viene elencato nelle pagine in cui vengono visualizzati gli avvisi ma non incide sullo stato di gravità del dispositivo applicabile.

Procedura

Per confermare un avviso, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi**. Verrà visualizzata la pagina Avvisi.

Passo 2. Selezionare gli avvisi da confermare.

Passo 3. Fare clic sull'icona **Avvisi confermati** ( ).

Al termine

- È possibile visualizzare un elenco di avvisi confermati dalla pagina Avvisi facendo clic sull'icona **Mostra avvisi esclusi/confermati** ( ) per visualizzare la finestra di dialogo Avvisi esclusi/confermati e facendo quindi clic sulla scheda **Avvisi confermati**.
- È possibile rimuovere la conferma di un avviso attivo facendo clic sull'icona **Mostra avvisi esclusi/confermati** ( ) per visualizzare la finestra di dialogo Avvisi esclusi/confermati, selezionando la scheda **Avvisi confermati**, scegliere gli avvisi e quindi fare clic sull'icona **Rimuovi conferma** ( ).

Utilizzo degli eventi

Da Lenovo XClarity Administrator è possibile accedere a un log eventi e a un log di controllo.

Informazioni su questa attività

Ulteriori informazioni: XClarity Administrator: monitoraggio

Il *log eventi* fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.

Il *log di controllo* fornisce un record cronologico degli interventi dell'utente, ad esempio il login a Lenovo XClarity Administrator, la creazione di un nuovo utente e la modifica di una password utente. È possibile utilizzare il log di controllo per tenere traccia e documentare l'autenticazione e i comandi nei sistemi IT.

Monitoraggio degli eventi nel log eventi

Il *log eventi* fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.

Informazioni su questa attività

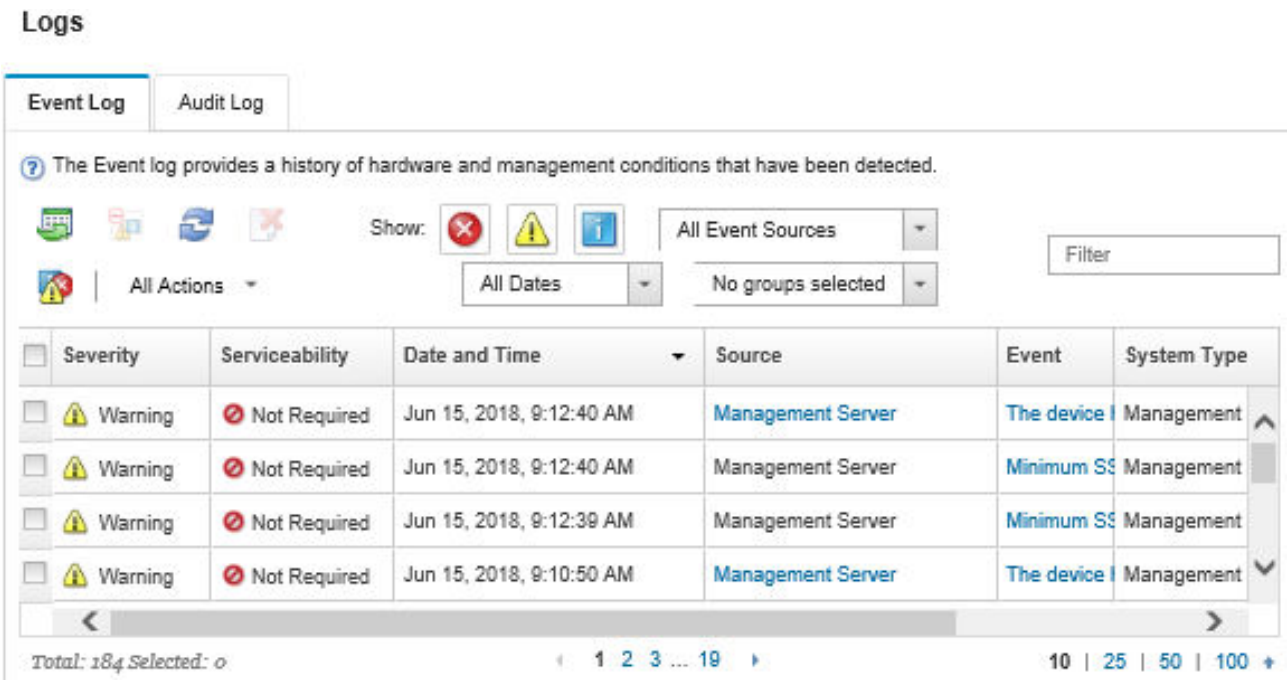
Il log eventi contiene gli eventi informativi e non informativi. Il numero di ciascuno di questi eventi varia finché non viene raggiunto il numero massimo di 50.000 eventi nel log eventi. In quel momento, si registra un massimo di 25.000 eventi informativi e 25.000 eventi non informativi. Inizialmente, ad esempio, nel log eventi sono presenti 0 eventi. Poniamo che vengano ricevuti 20.000 eventi informativi e 30.000 eventi non informativi. Quando viene ricevuto l'evento successivo, l'evento informativo meno recente viene rimosso se un evento non informativo è meno recente. Alla fine il log bilancia gli eventi al fine di contenere 25.000 eventi per ciascun tipo.

Lenovo XClarity Administrator invia un evento quando il log eventi raggiunge l'80% delle dimensioni minime e un altro evento quando la somma dell'evento e dei log di controllo raggiunge il 100% delle dimensioni massime.

Suggerimento: è possibile esportare il log eventi per assicurarsi di avere un record completo di tutti gli eventi hardware e di gestione. Per esportare il log eventi fare clic sull'icona **Esporta come CSV** ( ).

Procedura

Per visualizzare il log eventi, fare clic su **Monitoraggio → Log eventi** dalla barra dei menu di Lenovo XClarity Administrator, quindi sulla scheda **Log eventi**. Viene visualizzata la pagina Log eventi.



La colonna **Intervento richiesto** indica se il dispositivo richiede un intervento. Questa colonna può contenere uno dei seguenti valori:

- **Non richiesto**. L'evento è informativo e non richiede intervento.
- **Utente**. Intraprende l'azione di ripristino appropriata per risolvere il problema.

Per visualizzare le informazioni su un evento specifico, fare clic sul collegamento nella colonna **Evento**. Viene visualizzata una finestra di dialogo con informazioni sulle proprietà del dispositivo che ha inviato l'evento, i dettagli sull'evento e le azioni di ripristino.

- **Supporto**. Se Call Home è abilitato su Lenovo XClarity Administrator, l'evento verrà generalmente inoltrato al Centro assistenza clienti Lenovo a meno che non esista già un ticket di assistenza per lo stesso ID evento per il dispositivo.

  Se Call Home non è abilitato, si consiglia di aprire manualmente un ticket di assistenza per risolvere il problema (vedere Apertura di un ticket di assistenza nella documentazione online Lenovo XClarity Administrator).

Risultati

Dalla pagina Log eventi, procedere come segue:

- Visualizzare l'origine dell'evento facendo clic sul collegamento nella colonna **Origine**.
- Aggiornare l'elenco degli elenchi facendo clic sull'icona **Aggiorna** ( ).

  Suggerimento: il log eventi si aggiorna automaticamente ogni 30 secondi se vengono rilevati nuovi eventi.
- Cancella tutti gli eventi dal log eventi selezionando **Tutte le azioni → Cancella log eventi**.
- Visualizzare i dettagli su un evento specifico facendo clic sul collegamento nella colonna **Evento**, quindi sulla scheda **Dettagli**.
- Esportare il log eventi facendo clic sull'icona **Esporta come CSV** ( ).

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Escludere gli eventi specifici da tutte le pagine in cui vengono visualizzati gli eventi (vedere Esclusione di eventi).
- Restringere l'elenco degli eventi di gestione e hardware visualizzati nella pagina corrente:
  - Mostrare o nascondere gli eventi di una gravità specifica facendo clic sulle seguenti icone dall'elenco a discesa:
    - Icona **Eventi critici** ( )
    - Icona **Eventi di avvertenza** ( )
    - Icona **Eventi informativi** ( )
  - Mostrare solo eventi di fonti specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le origini avvisi
    - Eventi hardware
    - Eventi di gestione
    - Eventi di manutenzione
    - Eventi manutenibili cliente
    - Eventi non manutenibili
  - Mostrare solo gli eventi con una data e un'ora specifiche. É possibile scegliere una delle seguenti opzioni:
    - Tutte le date
    - 2 ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
    - Custom

Se si seleziona **Personalizzato**, è possibile filtrare gli eventi di gestione e hardware generati tra una data di avvio personalizzata e la data corrente.

- Elencare solo gli eventi che contengono testo specifico immesso nel campo **Filtro**.
- Ordinare gli eventi per colonna facendo clic sull'intestazione di una colonna.

Monitoraggio degli eventi nel log di controllo

Il *log di controllo* fornisce un record cronologico degli interventi dell'utente, ad esempio il login a Lenovo XClarity Administrator, la creazione di un nuovo utente e la modifica di una password utente. È possibile utilizzare il log di controllo per tenere traccia e documentare l'autenticazione e i comandi nei sistemi IT.

Informazioni su questa attività

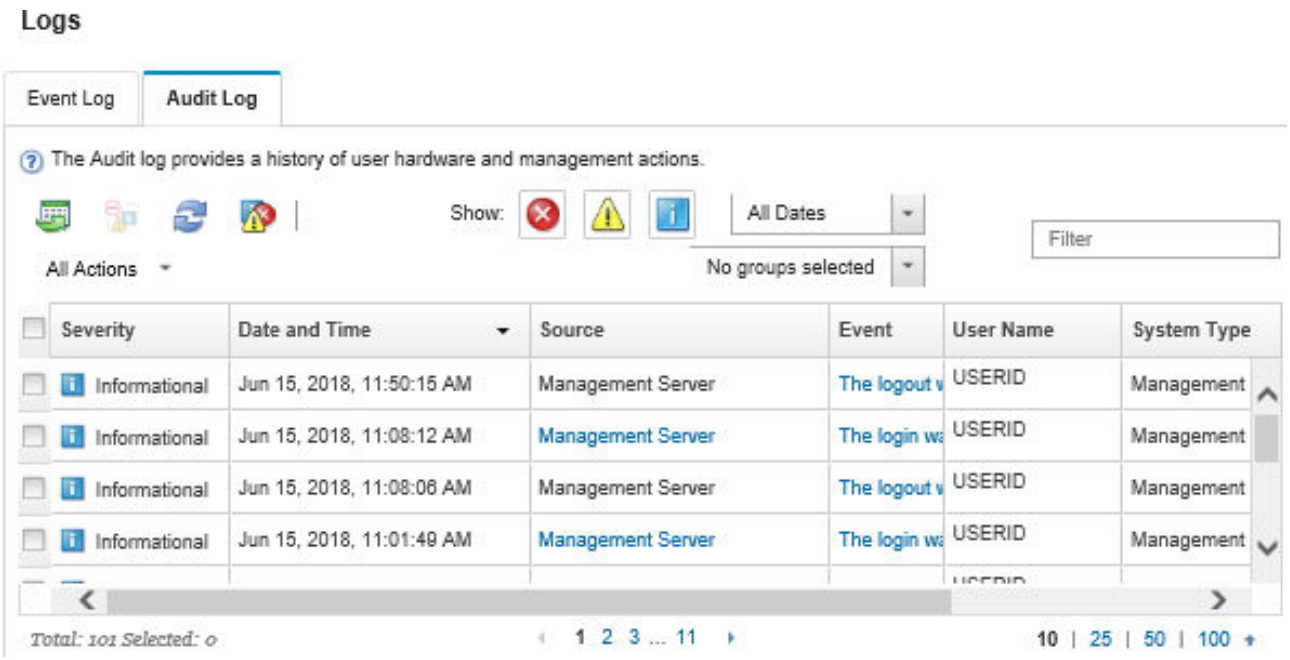
Il log di controllo può contenere un massimo di 50.000 eventi. Quando le dimensioni massime vengono raggiunte, l'evento meno recente nel log viene rimosso e il nuovo evento viene aggiunto al log.

XClarity Administrator invia un evento quando il log di controllo raggiunge l'80% delle dimensioni massime ed un altro evento quando la somma dell'evento e dei log di controllo raggiunge il 100% delle dimensioni massime.

Suggerimento: è possibile esportare il log di controllo per assicurarsi di avere un record completo di tutti gli eventi di controllo. Per esportare il log di controllo fare clic sull'icona **Esporta come CSV** ( ).

Procedura

Per visualizzare il log di controllo, fare clic su **Monitoraggio → Log eventi** dalla barra dei menu di XClarity Administrator, quindi sulla scheda **Log di controllo**. Viene visualizzata la pagina Log di controllo.



Per visualizzare le informazioni su un evento di controllo specifico, fare clic sul collegamento nella colonna **Evento**. Viene visualizzata una finestra di dialogo con informazioni sulle proprietà del dispositivo che ha inviato l'evento, i dettagli sull'evento e le azioni di ripristino.

Risultati

Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare l'origine dell'evento di controllo facendo clic sul collegamento nella colonna **Origine**.
- Aggiornare l'elenco degli eventi di controllo facendo clic sull'icona **Aggiorna** ( ).

  Suggerimento: il log eventi si aggiorna automaticamente ogni 30 secondi se vengono rilevati nuovi eventi.
- Visualizzare i dettagli su un evento di controllo specifico facendo clic sul collegamento nella colonna **Evento**, quindi sulla scheda **Dettagli**.
- Esportare il log di controllo facendo clic sull'icona **Esporta come CSV** ( ).

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Escludere eventi di controllo specifici da tutte le pagine in cui vengono visualizzati gli eventi (vedere Esclusione di eventi).
- Restringere l'elenco degli eventi di controllo visualizzati nella pagina corrente:
  - Mostrare o nascondere gli eventi di una gravità specifica facendo clic sulle seguenti icone:
    - Icona **Eventi critici** ( )
    - Icona **Eventi di avvertenza** ( )
    - Icona **Eventi informativi** ( )
  - Mostrare solo gli eventi con una data e un'ora specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le date
    - 2 ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
    - Custom

    Se si seleziona **Personalizzato**, è possibile filtrare gli eventi di gestione e hardware generati tra una data di avvio personalizzata e la data corrente.
  - Elencare solo gli eventi che contengono testo specifico immesso nel campo **Filtro**.
  - Ordinare gli eventi per colonna facendo clic sull'intestazione di una colonna.

Risoluzione di un evento

Lenovo XClarity Administrator fornisce informazioni sulle azioni appropriate da eseguire per risolvere un evento.

Procedura

Per risolvere un evento, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Log eventi** per visualizzare la pagina Log.

Passo 2. Fare clic sulla scheda **Log eventi**.

Passo 3. Individuare l'evento nel log eventi.

Passo 4. Per visualizzare le informazioni sull'evento (incluse le azioni di ripristino e una spiegazione) e sul dispositivo che lo ha generato, fare clic sul collegamento nella colonna **Evento**.

Passo 5. Fare clic sulla scheda **Dettagli**.

Passo 6. Completare le azioni di ripristino nella scheda **Dettagli** per risolvere l'evento.

> **Nota:** se la spiegazione e l'azione di ripristino per un evento non vengono visualizzate, visitare il Documentazione online di Lenovo Flex System e cercare il titolo dell'evento. Nel sito Web sono sempre disponibili le informazioni più aggiornate.
>
> Se, dopo essersi attenuti alla procedura consigliata, il problema persiste, contattare il Supporto Lenovo.

Esclusione di eventi

Se vengono visualizzati eventi che non interessano l'utente, è possibile escludere tali eventi da tutte le pagine in cui vengono visualizzati. Gli eventi esclusi compaiono ancora nel log ma vengono nascosti da tutte le pagine in cui sono visualizzati.

Informazioni su questa attività

Gli eventi esclusi vengono nascosti per tutti gli utenti, non solo per l'utente che imposta la configurazione.

È possibile impostare i dispositivi in modalità di manutenzione, in modo da escludere tutti gli eventi e gli avvisi relativi a questi dispositivi (vedere Impostazione dei dispositivi in modalità di manutenzione).

Restrizione: solo gli utenti con privilegi di amministratore possono escludere o ripristinare gli eventi.

Procedura

Per escludere gli eventi dal log eventi, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Log eventi**, quindi su **Log eventi**. Viene visualizzata la finestra di dialogo Log eventi.

Passo 2. Selezionare gli eventi da escludersi e fare clic sull'icona **Escludi eventi** ( ). Viene visualizzata la finestra di dialogo Escludi eventi.

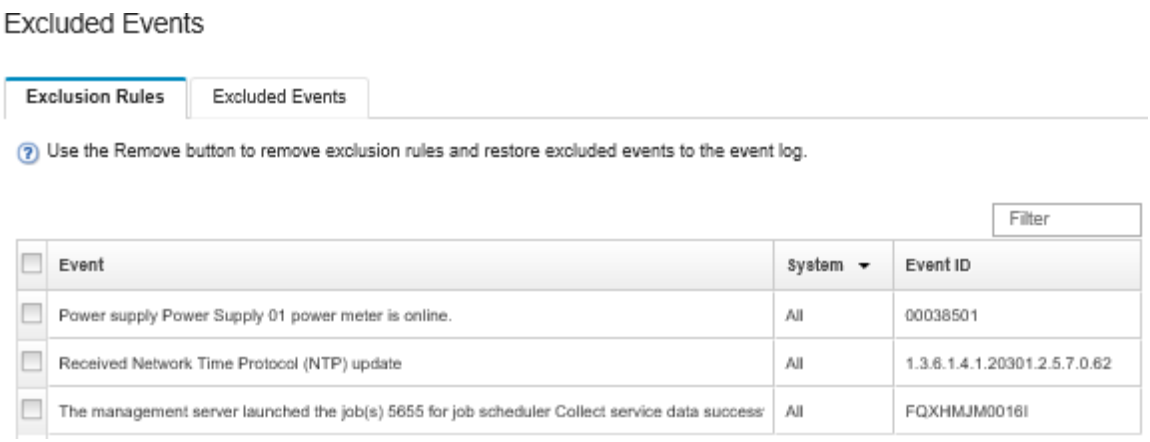
Passo 3. Selezionare una delle seguenti opzioni:
- **Escludi eventi selezionati da tutti i sistemi**. Esclude gli eventi selezionati da tutti i dispositivi gestiti.
- **Escludi eventi solo dai sistemi nell'ambito dell'istanza selezionata**. Esclude gli eventi selezionati dai dispositivi gestiti a cui si applicano.

Passo 4. Fare clic su **Salva**.

Al termine

Quando si escludono gli eventi, Lenovo XClarity Administrator crea regole di esclusione in base alle informazioni fornite.

- Visualizza un elenco di regole di esclusione e di eventi esclusi dalla pagina Log facendo clic sull'icona **Mostra eventi esclusi** ( ). Nella finestra di dialogo Eventi esclusi, fare clic sulla scheda **Regole di esclusione** per visualizzare le regole di esclusione oppure sulla scheda **Eventi esclusi** per visualizzare gli eventi esclusi.



- Ripristina gli eventi esclusi nel log eventi rimuovendo la regola di esclusione appropriata. Per rimuovere una regola di esclusione, fare clic sull'icona **Mostra eventi esclusi** icon ( ) per visualizzare la finestra di dialogo Eventi esclusi, selezionare le regole di esclusione da ripristinare, quindi fare clic su **Rimuovi esclusioni**.
- Prevenire che gli eventi che richiedono assistenza presenti nell'elenco degli eventi esclusi aprano automaticamente i report dei problemi, facendo clic su **Amministrazione → Assistenza e supporto** dalla barra dei menu di Lenovo XClarity Administrator, facendo clic sulla scheda **Server d'inoltro di servizio** e quindi selezionando **No** accanto alla domanda **Si desidera che gli eventi esclusi aprano i report dei problemi?**.

Inoltro di eventi

È possibile configurare Lenovo XClarity Administrator affinché inoltri gli eventi ai dispositivi mobili e alle applicazioni collegate nel proprio ambiente per aggregare e monitorare lo stato dell'hardware e i problemi di runtime per l'ambiente hardware.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Inoltro di eventi a syslog, a un programma di gestione SNMP remoto e ad altri servizi di eventi

È possibile configurare Lenovo XClarity Administrator affinché inoltri gli eventi alle applicazioni collegate nel proprio ambiente per aggregare e monitorare lo stato dell'hardware e i problemi di runtime per l'ambiente hardware. È possibile definire l'ambito degli eventi da inoltrare in base al dispositivo, alla classe dell'evento, alla gravità dell'evento e al componente.

Informazioni su questa attività

Lenovo XClarity Administrator può inoltrare gli eventi per uno o più dispositivi. Per gli eventi di controllo, è possibile scegliere di inoltrare tutti gli eventi di controllo o nessuno. Non è possibile inoltrare eventi di controllo specifici. Per gli eventi di gestione e hardware, è possibile scegliere di inoltrare gli eventi per una o più gravità (eventi critici, di avvertenza e informativi) e per uno o più componenti (unità disco, processori e adattatori).

Lenovo XClarity Administrator utilizza i server d'inoltro degli eventi per inoltrare gli eventi. Un *server d'inoltro degli eventi* include le informazioni sul protocollo da utilizzare, sul destinatario, sui dispositivi da monitorare e sugli eventi da inoltrare. Dopo aver creato e abilitato un server d'inoltro degli eventi, Lenovo XClarity Administrator avvia il monitoraggio per gli eventi in entrata in base ai criteri del filtro. Quando viene rilevata una corrispondenza, per inoltrare l'evento viene utilizzato il protocollo associato.

Sono supportati i seguenti protocolli:

- **Azure Log Analytics**. Lenovo XClarity Administrator inoltra gli eventi monitorati in rete a Microsoft Azure Log Analytics.
- **E-mail**. Lenovo XClarity Administrator inoltra gli eventi monitorati ad uno o più indirizzi e-mail mediante SMTP. L'e-mail contiene informazioni sull'evento, il nome host del dispositivo sorgente e i collegamenti all'interfaccia Web di Lenovo XClarity Administrator e all'app Lenovo XClarity Mobile.
- **FTP**. Inoltra gli eventi monitorati in rete a un server FTP.
- **REST**. Lenovo XClarity Administrator inoltra gli eventi monitorati in rete a un Web Service REST.
- **SNMP**. Lenovo XClarity Administrator inoltra gli eventi monitorati sulla rete ad un programma di gestione SNMP remoto. I trap SNMPv1 e SNMPv3 sono supportati.

  Per informazioni sul file MIB (Management Information Base) che descrive i trap SNMP generati da Lenovo XClarity Administrator, vedere file lenovoMgrAlert.mib nella documentazione online di Lenovo XClarity Administrator.
- **Syslog**. Lenovo XClarity Administrator inoltra gli eventi monitorati sulla rete a un server log centrale in cui gli strumenti nativi possono essere utilizzati per monitorare il syslog.

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Nota: Gli eventi non vengono recapitati se, ad esempio, la connettività tra Lenovo XClarity Administrator e il server d'inoltro degli eventi è interrotta o se la porta è bloccata.

Configurazione dell'inoltro eventi a Azure Log Analytics

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a Azure Log Analytics.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per Azure Log Analytics.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **Azure Log Analytics** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome e la descrizione facoltativa per il server d'inoltro degli eventi.
- Immettere la chiave primaria per l'interfaccia Azure Log Analytics.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo**: se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Base**. Esegue l'autenticazione server specificato utilizzando l'ID utente e la password specificati.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari Azure Log Analytics. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari Azure Log Analytics sono elencate nella finestra di dialogo Formato di output.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un

dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I,FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

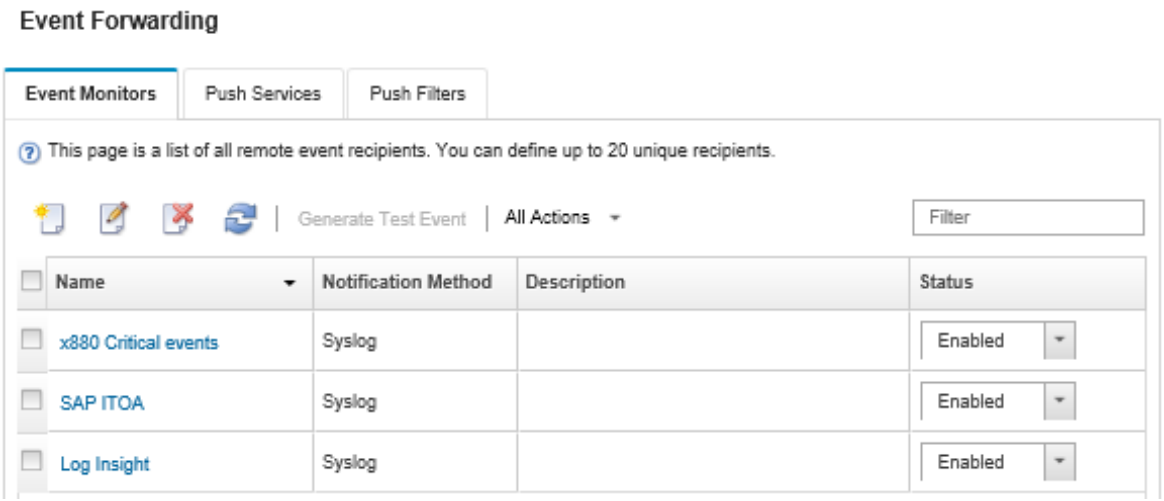
1. Utilizzare le icone **Scorri a sinistra** (◄) e **Scorri a destra** (►) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.

3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al server Azure Log Analytics appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).

- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro degli eventi a un servizio di posta elettronica mediante il protocollo SMTP

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un servizio di posta elettronica utilizzando il protocollo SMTP.

Prima di iniziare

Per inoltrare l'e-mail a un servizio e-mail basato sul Web (ad esempio Gmail, Hotmail o Yahoo), il server SMTP deve supportare l'inoltro della posta elettronica Web.

Prima di configurare un server di inoltro degli eventi su un servizio Web di Gmail consultare le informazioni in Configurazione dell'inoltro eventi a syslog, a un programma di gestione SNMP remoto o a un'e-mail nella documentazione online di Lenovo XClarity Administrator.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per la posta elettronica mediante SMTP.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **E-mail** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per il server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `25`.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- Immettere l'indirizzo e-mail per ciascun destinatario. Separare gli indirizzi e-mail con una virgola.

  Per inviare e-mail al contatto del supporto assegnato per il dispositivo, selezionare **Usa e-mail contatto del supporto** (vedere Definizione dei contatti di supporto per un dispositivo nella documentazione online di XClarity Administrator).
- **Facoltativo:** immettere l'indirizzo e-mail del mittente dell'e-mail (ad esempio, `john@company.com`).

Se non viene specificato un indirizzo e-mail, l'indirizzo del mittente è `LXCA.<source_identifier>@<smtp_host>` per impostazione predefinita.

Se viene specificato solo il dominio del mittente, il formato dell'indirizzo del mittente è *<LXCA_host_name>@<sender_domain>* (ad esempio, XClarity1@company.com).

Note:

- Se si configura un server SMTP affinché richieda un nome host per l'inoltro delle e-mail e non si configura un nome host per XClarity Administrator, è possibile che il server SMTP rifiuti gli eventi inoltrati. Se XClarity Administrator non dispone di un nome host, l'evento viene inoltrato con l'indirizzo IP. Se l'indirizzo IP non può essere ottenuto, verrà inviato "localhost". Ciò potrebbe far sì che il server SMTP rifiuti l'evento.
- Se viene specificato il dominio del mittente, la fonte non si identifica nell'indirizzo del mittente. Vengono, invece, incluse le informazioni sulla fonte dell'evento nel corpo dell'e-mail, tra cui il nome di sistema, l'indirizzo IP, il tipo o il modello e il numero di serie.
- Se il server SMTP accetta solo le e-mail inviate da un utente registrato, l'indirizzo predefinito del mittente (`LXCA.<source_identifier>@<smtp_host>`) viene rifiutato. In questo caso, è necessario specificare almeno un nome di dominio nel campo **Indirizzo di provenienza**.

- **Facoltativo:** per stabilire una connessione protetta al server SMTP, selezionare i seguenti tipi di connessione:
  - **SSL**. Utilizzare il protocollo SSL durante la comunicazione.
  - **STARTTLS**. Utilizzare il protocollo TLS per formare una comunicazione protetta su un canale non protetto.

  Se viene selezionato uno di questi tipi di connessione, LXCA tenta di scaricare e importare il certificato del server SMTP nel proprio archivio attendibile. All'utente verrà richiesto di accettare l'aggiunta di questo certificato nell'archivio attendibile.
- **Facoltativo:** se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Regolare**. Esegue l'autenticazione server SMTP specificato utilizzando l'ID utente e la password specificati.
  - **NTLM**. Utilizza il protocollo NT LAN Manager (NTLM) per eseguire l'autenticazione al server SMTP specificato utilizzando l'ID utente, la password e il nome di dominio specificati.
  - **OAUTH2**. Utilizza il protocollo Simple Authentication and Security Layer (SASL) per eseguire l'autenticazione al server SMTP specificato utilizzando il nome utente e il token di sicurezza specificati. Generalmente, il nome utente è l'indirizzo e-mail.

    Attenzione: il token di sicurezza scade dopo un breve periodo di tempo. L'aggiornamento del token di sicurezza è responsabilità dell'utente.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare nel corpo dell'e-mail e il formato dell'oggetto dell'e-mail. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari dell'e-mail. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari dell'e-mail sono elencate nella finestra di dialogo Formato output.

Oggetto dell'e-mail

```
[[DeviceName]]-[[EventMessage]]
```

Corpo dell'e-mail

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
```

```
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.

3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I,FQXHMEM0214I`).

- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.
- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

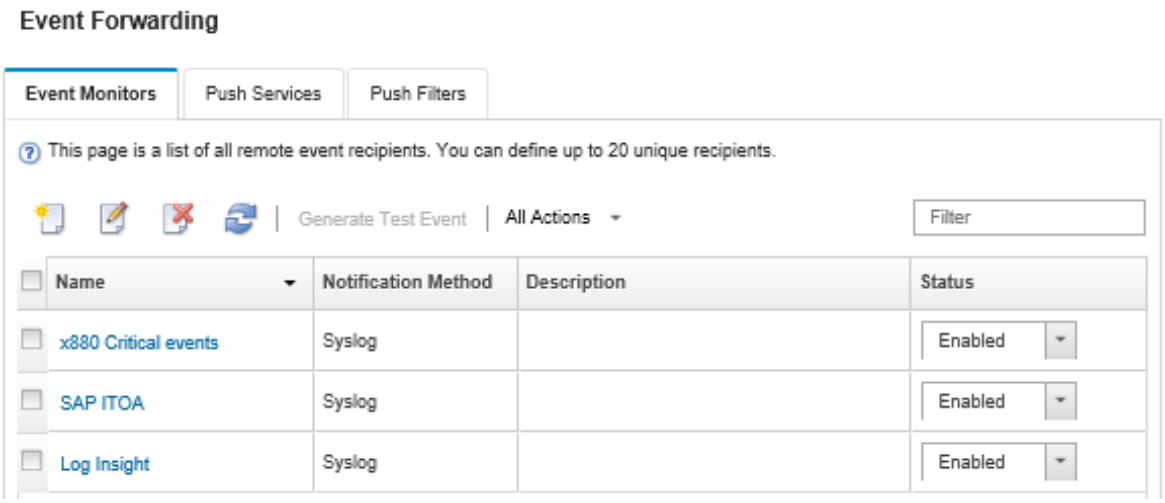
1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.

- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al servizio di posta elettronica appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un servizio SMTP Gmail

É possibile configurare Lenovo XClarity Administrator affinché inoltri eventi monitorati a un servizio e-mail basato su Web, come ad esempio Gmail.

Utilizzare i seguenti esempi di configurazione per impostare il server d'inoltro degli eventi affinché utilizzi il servizio SMTP di Gmail.

Nota: Gmail consiglia di utilizzare il metodo di autenticazione OAUTH2 per comunicazioni più sicure. Se si sceglie di utilizzare l'autenticazione regolare, verrà inviata un'e-mail per indicare che un'applicazione ha tentato di utilizzare l'account senza gli standard di sicurezza più recenti. Il messaggio include le istruzioni per la configurazione dell'account e-mail affinché accetti questi tipi di applicazioni.

Per informazioni sulla configurazione di un server SMTP di Gmail, vedere https://support.google.com/a/answer/176600?hl=en.

Autenticazione regolare mediante SSL sulla porta 465

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo SSL sulla porta 465 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	465
SSL	Seleziona
STARTTLS	Cancella
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione regolare mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancella
STARTTLS	Seleziona
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione OAUTH2 mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e un token di sicurezza Gmail validi.

Utilizzare la seguente procedura di esempio per ottenere il token di sicurezza.

1. Creare un progetto in Google Developers Console e recuperare l'ID e il client secret. Per ulteriori informazioni, visitare il sito Web Pagina Web per l'accesso di Google ai siti Web.
   a. Da un browser Web, aprire la Pagina Web delle API Google.

b. Dal menu di quella pagina Web, fare clic su **Seleziona un progetto → Crea progetto**. Viene visualizzata la finestra di dialogo Nuovo progetto.

c. Immettere un nome, selezionare **Sì** per accettare l'accordo di licenza e fare clic su **Crea**.

d. Nella scheda **Panoramica**, utilizzare il campo di ricerca per cercare "gmail".

e. Fare clic su **GMAIL API** nei risultati della ricerca.

f. Fare clic su **Abilita**.

g. Fare clic sulla scheda **Credenziali**.

h. Fare clic su **Schermata consenso OAuth**.

i. Immettere un nome nel campo **Nome del prodotto visualizzato dagli utenti** e fare clic su **Salva**.

j. Fare clic su **Crea credenziali → ID client OAuth**.

k. Selezionare **Altro** e immettere un nome.

l. Fare clic su **Crea**. Viene visualizzata la finestra di dialogo Client OAuth con l'ID e il segreto client.

m. Prendere nota dell'ID e del segreto client per utilizzarli in futuro.

n. Fare clic su **OK** per chiudere la finestra di dialogo.

2. Utilizzare lo script Phyton oauth2.py per generare e autorizzare un token di sicurezza fornendo l'ID e il segreto client generato al momento della creazione del progetto.

   Nota: per completare questa operazione è necessario Python versione 2.7. È possibile scaricare ed installare Python 2.7 dal Sito Web di Python.

   a. Da un browser Web, aprire la Pagina Web gmail-oauth2-tools.

   b. Fare clic su **Non elaborato** e salvare il contenuto in un file denominato `oauth2.py` sul sistema locale.

   c. Eseguire il seguente comando come terminale (Linux) o come riga di comando (Windows):

   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```

   Ad esempio

   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```

   Questo comando restituisce un URL da utilizzare per autorizzare il token e per recuperare un codice di verifica dal sito Web di Google, ad esempio:

   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
   google.com%2F

   Enter verification code:
   ```

   d. Da un browser Web, aprire l'URL che è stato restituito nel passaggio precedente.

   e. Fare clic su **Consenti** per accettare questo servizio. Viene restituito un codice di verifica.

   f. Immettere il codice di verifica nel comando `oauth2.py`.

   Il comando restituisce il token di sicurezza e aggiorna il token, ad esempio:

   ```
   Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
   Access Token Expiration Seconds: 3600
   ```

Importante: il token di sicurezza scade dopo un periodo di tempo. È possibile utilizzare lo script Phyton oauth2.py e il token di aggiornamento per generare un nuovo token di sicurezza. La generazione del nuovo token di sicurezza e l'aggiornamento del server di inoltro degli eventi tramite il nuovo token in Lenovo XClarity Administrator è responsabilità dell'utente.

3. Dall'interfaccia Web di Lenovo XClarity Administrator, configurare il server di inoltro degli eventi per e-mail utilizzando i seguenti attributi:

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancella
STARTTLS	Seleziona
Autenticazione	OAUTH2
Utente	Indirizzo e-mail Gmail valido
Token	Token di sicurezza
Indirizzo di provenienza	(facoltativo)

Configurazione dell'inoltro di eventi a un server FTP

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un server FTP.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un server FTP.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **FTP** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per i server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 21.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.

- **Facoltativo:** specificare la sequenza di caratteri da rimuovere dal contenuto del file.
- Immettere il formato del nome file da utilizzare per il file che contiene l'evento inoltrato. Il formato predefinito è `event_[[EventSequenceID]].txt`.

  Nota: Ogni file contiene le informazioni per un singolo evento.
- Immettere il percorso del server FTP remoto su cui il file deve essere caricato.
- Scegliere la codifica dei caratteri: **UTF 8** o **Big5**. L'impostazione predefinita è UTF-8.
- Selezionare il tipo di autenticazione. É possibile selezionare uno dei seguenti valori.
  - **Anonimo**. (predefinito) Non viene utilizzata alcuna autenticazione
  - **Base**. Esegue l'autenticazione sul server FTP utilizzando l'ID utente e la password specificati.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari FTP. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari FTP sono elencate nella finestra di dialogo Formato output.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n"
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

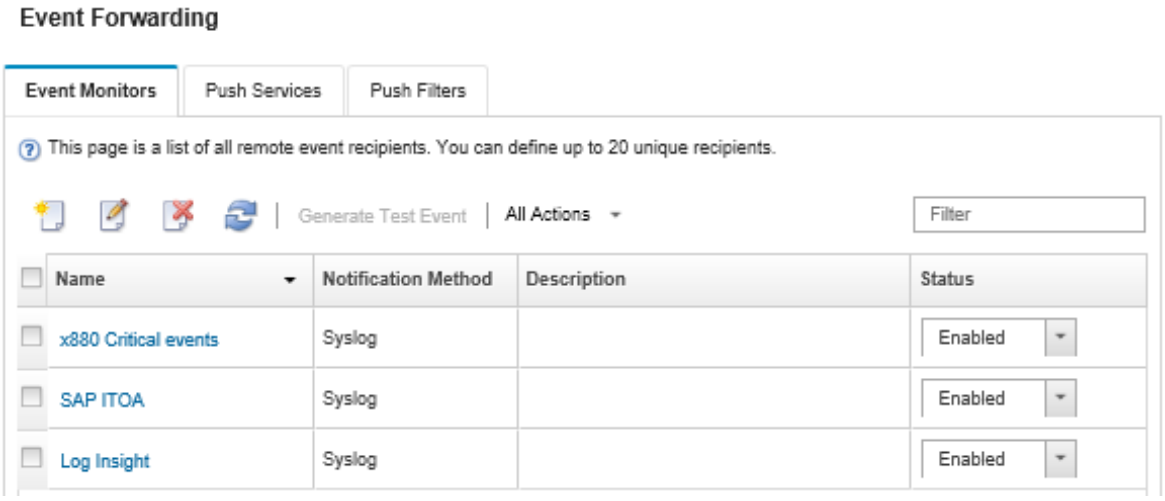
1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:

- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al server FTP appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un servizio Web REST

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un servizio Web REST.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un servizio Web REST.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **REST** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il percorso della risorsa in cui il server d'inoltro pubblicherà gli eventi (ad esempio, /rest/test).
- Selezionare il protocollo da utilizzare per l'inoltro di eventi. É possibile selezionare uno dei seguenti valori.
  - **HTTP**
  - **HTTPS**
- Selezionare il metodo REST. É possibile selezionare uno dei seguenti valori.
  - **PUT**
  - **POST**
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.

- **Facoltativo:** se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Base**. Esegue l'autenticazione server specificato utilizzando l'ID utente e la password specificati.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari del servizio Web REST. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari del servizio Web REST sono elencate nella finestra di dialogo Formato output.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.

4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).

- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.
- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

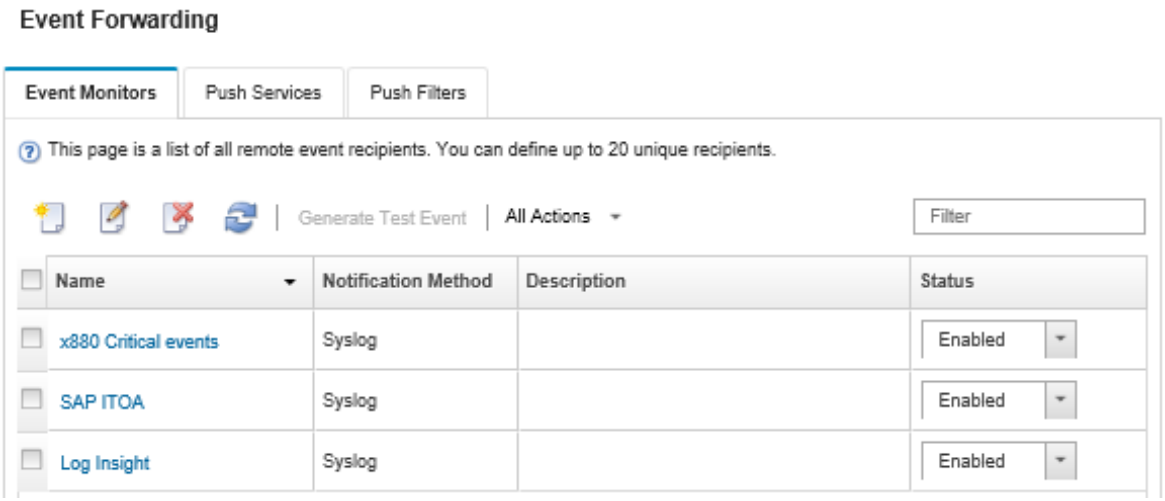
1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.

- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al servizio Web REST appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un gestore SNMPv1 o SNMPv3 remoto

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un gestore SNMPv1 o SNMPv3 remoto.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Per informazioni sull'utilizzo di MIB per XClarity Administrator, vedere file lenovoMgrAlert.mib.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un gestore SNMPv1 o SNMPv3 remoto.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **SNMPv1** o **SNMPv3** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome e la destinazione host per il server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `162`.
- **Facoltativo:** immettere le informazioni aggiuntive, ad esempio la descrizione, il nome del contatto e la posizione.
- Selezionare la versione SNMP. É possibile selezionare uno dei seguenti valori.
  - **SNMPv1**. Se viene selezionata questa versione, specificare la password della comunità inviata con ogni richiesta SNMP al dispositivo.
  - **SNMPv3**. Questa è la versione predefinita ed è consigliata per una protezione avanzata. Se è selezionata l'opzione SNMPv3, specificare, opzionalmente, l'ID utente, il tipo e la password di autenticazione e il tipo di privacy e la relativa password.

    Se il ricevitore trap SNMPv3 richiede l'ID del motore per l'istanza XClarity Administrator, è possibile individuare l'ID del motore eseguendo le seguenti operazioni:

    1. Verificare che i parametri della connessione (username, authProtocol, authPassword, privProtocol, privPassword) corrispondano a quelli configurati in XClarity Administrator.
    2. Utilizzando il software preferito (ad esempio snmpwalk), eseguire una richiesta GET SNMP sul server XClarity Administrator utilizzando uno dei seguenti OID:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

       Utilizzare la seguente sintassi per eseguire questo comando `snmpget`. Il tipo di autenticazione del server d'inoltro -a può essere SHA o vuoto (nessuna autenticazione).
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_
       ```

       Ad esempio, se l'indirizzo IP di XClarity Administrator è 192.0.1.0, il tipo di autenticazione è SHA e il tipo di privacy è AES, il comando che segue mostra l'ID del motore.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1
       ```

       Viene restituita la seguente risposta di esempio. In questo esempio l'ID del motore è 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.

- **Facoltativo**: se è necessaria l'autenticazione trap, immettere l'ID utente e la password di autenticazione. È necessario immettere lo stesso ID utente e password per il gestore SNMP remoto a cui sono stati inoltrati i trap.
- Selezionare il protocollo di autenticazione utilizzato dal gestore SNMP remoto per verificare il mittente del trap. É possibile selezionare uno dei seguenti valori
  - **SHA**. Utilizza il protocollo SHA per eseguire l'autenticazione al server SNMP specificato utilizzando l'ID utente, la password e il nome di dominio specificati.
  - **Nessuna**. Non viene utilizzata alcuna autenticazione
- Se è necessaria la crittografia del trap, immettere il tipo di privacy (protocollo di crittografia) e la password. É possibile selezionare uno dei seguenti valori. È necessario immettere lo stesso protocollo e password per il gestore SNMP remoto a cui sono stati inoltrati i trap.
  - **AES**
  - **DES**
  - **Nessuno**

Passo 5. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 6. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 7. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 8. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 9. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 10. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I,FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.

4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.

- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 11. Scegliere se includere determinati tipi di eventi.
- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 12. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 13. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 14. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 15. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

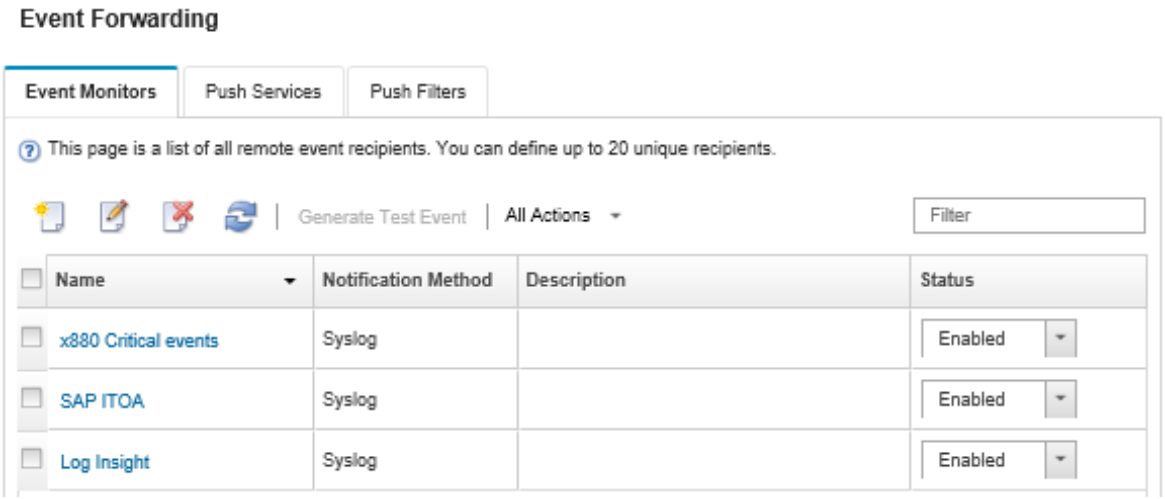
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 16. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 17. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al gestore SNMP remoto appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).
- Scaricare il file MIB contenente informazioni sui trap SNMP facendo clic sull'icona **Crea** ( ), quindi selezionando **Scarica file MIB** nella scheda Generale della finestra di dialogo Nuovo server d'inoltro eventi.

file lenovoMgrAlert.mib

Questo file MIB (Management Information Base) descrive i trap SNMP generati da Lenovo XClarity Administrator, inclusi gli avvisi generati da XClarity Administrator e dai dispositivi gestiti. È possibile compilare questo file MIB in qualsiasi programma di gestione SNMP in modo che i trap SNMP inviati da XClarity Administrator possano essere visualizzati significativamente.

È possibile scaricare il file MIB dall'interfaccia Web facendo clic su **Monitoraggio → Inoltro eventi** sulla barra dei menu, quindi sull'icona **Crea** ( ), selezionando **SNMP** per il tipo di server d'inoltro degli eventi e facendo clic su **Scarica file MIB** nella parte inferiore della finestra di dialogo.

I seguenti oggetti sono inclusi in tutti i trap SNMP in uscita. Gli oggetti aggiuntivi potrebbero essere inclusi in alcuni trap SNMP. Tutti gli oggetti sono descritti nel file MIB. Le informazioni di ripristino non sono incluse nel trap.

Nota: Questo elenco potrebbe differire da una versione di XClarity Administrator a un'altra.
- **mgrTrapAppId**. "Lenovo Event Manager".
- **mgrTrapCommonEvtID**. ID dell'evento comune

- **mgrTrapDateTime**. Data e ora locali in cui è stato generato l'evento
- **mgrTrapEventClass**. L'origine dell'evento. controllo, raffreddamento, alimentazione, dischi, memoria, processori, sistema, test, adattatore, espansione, modulo I/O o blade.
- **mgrTrapEvtID**. Identificativo univoco dell'evento
- **mgrTrapFailFRUs**. Elenco separato da virgola degli UUID FRU non validi, se applicabile
- **mgrTrapFailSNs**. Elenco separato da virgola dei numeri di serie per le FRU non valide, se applicabile.
- **mgrTrapFullyQualifiedDomainName**. Nome completo di dominio: il nome host e il nome di dominio.
- **mgrTrapID**. Trap ID
- **mgrTrapMsgText**. Testo del messaggio (solo inglese).
- **mgrTrapMsgID**. Identificativo del messaggio.
- **mgrTrapMtm**. Modello del tipo di modello del dispositivo che ha generato l'evento
- **mgrTrapService**. Indicatore dell'intervento richiesto: 000 (sconosciuto), 100 (nessuno), 200 (centro di assistenza) o 300 (cliente)
- **mgrTrapSeverity**. Indicatore della gravità: informativo, avvertenza, minore, principale o critico
- **mgrTrapSN**. Numero di serie del dispositivo che ha generato l'evento.
- **mgrTrapSrcIP**. Indirizzo IP del dispositivo da cui si è ricevuto l'evento.
- **mgrTrapSrcLoc**. Posizione del dispositivo che ha generato l'evento, solo in inglese (ad esempio, Slot xx)
- **mgrTrapSrcName**. Nome host o nome visualizzato del dispositivo che ha generato l'evento.
- **mgrTrapSysContact**. ID di contatto configurato dall'utente.
- **mgrTrapSysLocation**. Informazioni sulla posizione del dispositivo configurato dall'utente.
- **mgrTrapSystemName**. Nome del dispositivo, nome del componente e posizione dello slot.
- **mgrTrapTxtId**. Nome host o indirizzo IP del server Lenovo Event Manager che ha generato il trap.
- **mgrTrapUserid**. ID utente associato all'evento (se l'evento è interno e la classe dell'evento è Controllo)
- **mgrTrapUuid**. UUID del dispositivo che ha generato l'evento.

Configurazione dell'inoltro eventi a un syslog

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un syslog.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un syslog.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **syslog** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per il server d'inoltro degli eventi.

- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `514`.
- Selezionare il protocollo da utilizzare per l'inoltro di eventi. É possibile selezionare uno dei seguenti valori.
  - **UDP**
  - **TCP**
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- Facoltativamente, selezionare il formato data/ora del syslog. É possibile selezionare uno dei seguenti valori.
  - **Ora locale**. Il formato predefinito, ad esempio `Fri Mar 31 05:57:18 EDT 2017`.
  - **Ora GMT**. Standard internazionale (ISO8601) per la data e l'ora, ad esempio `2017-03-31T05:58:20-04:00`.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari sylog. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari syslog sono elencate nella finestra di dialogo Formato output.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Selezionare **Consenti eventi esclusi** per impedire l'inoltro di eventi esclusi oppure deselezionare **Consenti eventi esclusi** per inoltrare eventi esclusi. Per ulteriori informazioni, vedere Esclusione di eventi.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Associa per categoria evento**
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.

4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).

- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.
- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

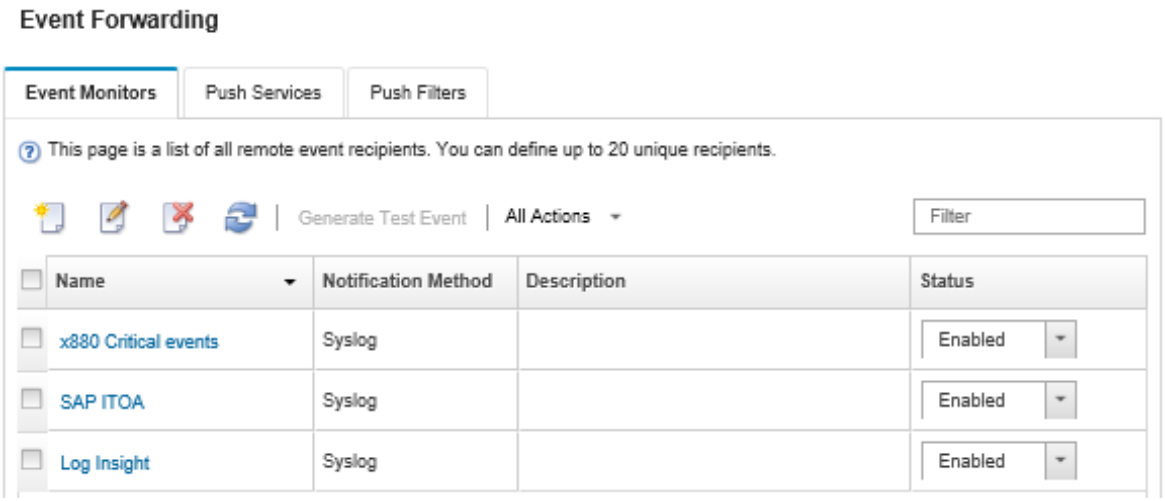
1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.

- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al syslog appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Sospensione dell'inoltro eventi

È possibile sospendere l'inoltro eventi disabilitando il server d'inoltro eventi. La sospensione dell'inoltro eventi interrompe il monitoraggio degli eventi in entrata. Gli eventi ricevuti al momento della sospensione del monitoraggio non vengono inoltrati.

Informazioni su questa attività

Lo stato Disabilitato non è permanente. Se il nodo di gestione viene riavviato, tutti i server d'inoltro degli eventi vengono abilitati.

Procedura

Attenersi alla procedura descritta di seguito per disabilitare l'inoltro di eventi.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Selezionare **Disabilita** nella colonna **Stato** per ciascun server d'inoltro degli eventi che si desidera sospendere.

Inoltro di eventi a dispositivi mobili

È possibile configurare Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi ai dispositivi mobili

Prima di iniziare

Per inoltrare gli eventi ai dispositivi mobili devono essere soddisfatti i seguenti requisiti:

- Verificare che un server DNS valido sia configurato per consentire a Lenovo XClarity Administrator di collegarsi ai server push Apple o Google. Il server può essere configurato facendo clic su **Amministrazione → Accesso alla rete → Modifica accesso alla rete** , quindi facendo clic sulla scheda **Impostazioni Internet** (vedere Configurazione dell'accesso alla rete nella documentazione online di Lenovo XClarity Administrator).
- Verificare che tutte le porte necessarie per la gestione degli eventi siano aperte sulla rete e sui firewall. Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di Lenovo XClarity Administrator.

Informazioni su questa attività

Quando l'app Lenovo XClarity Mobile è installata su un dispositivo mobile, è possibile abilitare ogni istanza collegata di Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi al dispositivo mobile selezionato. Quando le notifiche push sono abilitate per un'istanza specifica, viene creata una sottoscrizione in Lenovo XClarity Administrator per il dispositivo mobile selezionata.

È possibile definire gli eventi di cui è stato eseguito il push nel dispositivo mobile assegnando filtri eventi globali predefiniti o personalizzati per ciascuna istanza di Lenovo XClarity Administrator. I filtri eventi globali sono abilitati per impostazione predefinita. Lenovo XClarity Administrator avvia il monitoraggio degli eventi in entrata in base ai criteri dei filtri. Quando viene rilevata una corrispondenza, l'evento viene inoltrato al dispositivo mobile.

Per ulteriori informazioni su Lenovo XClarity Mobile e sui dispositivi mobili supportati, vedere Utilizzo di Lenovo XClarity Mobile nella documentazione online di Lenovo XClarity Administrator.

Procedura

Per configurare le notifiche push sul dispositivo mobile selezionato, attenersi alla procedura descritta di seguito dall'app Lenovo XClarity Mobile sul dispositivo mobile.

Passo 1. Abilitare le notifiche push:

- È possibile abilitare le notifiche push quando si crea una connessione ad un'istanza Lenovo XClarity Administrator. Le notifiche push sono abilitate per impostazione predefinita.
- È possibile abilitare le notifiche push sulle connessioni esistenti abilitando uno o più filtri eventi

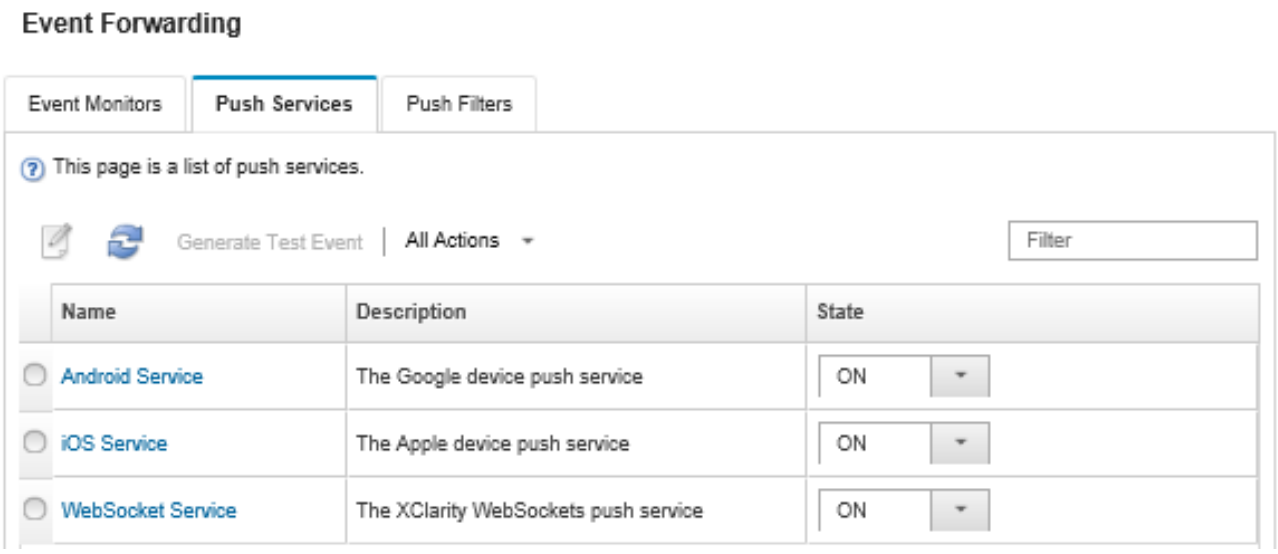
Passo 2. Assegnare i filtri eventi globali per specificare gli eventi che devono essere inoltrati al dispositivo mobile:

Nota: è possibile aggiungere o rimuovere i filtri eventi globali dalla sottoscrizione solo dall'app Lenovo XClarity Mobile. È possibile creare i filtri eventi globali solo dall'interfaccia Web Lenovo XClarity Administrator. Per informazioni sulla creazione di filtri eventi globali personalizzati, vedere Creazione di filtri eventi per dispositivi mobili e WebSockets.

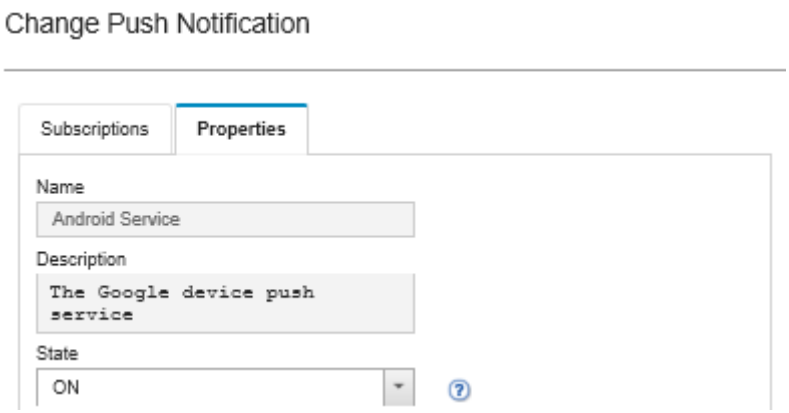
1. Toccare **Impostazioni → Notifiche push**. Viene visualizzato un elenco di connessioni Lenovo XClarity Administrator.
2. Toccare l'istanza Lenovo XClarity Administrator per visualizzare un elenco di filtri push.
3. Abilitare i filtri eventi per gli eventi di cui si desidera eseguire il push sul dispositivo mobile per l'istanza Lenovo XClarity Administrator.
4. Toccare **Tocca per generare notifica push di prova** per verificare che il push delle notifiche degli eventi venga eseguito correttamente.

Risultati

È possibile gestire le sottoscrizioni dalla pagina Inoltro eventi nell'interfaccia Web di Lenovo XClarity Administrator. Fare clic su **Monitoraggio → Inoltro eventi** per visualizzare la pagina Inoltro eventi.



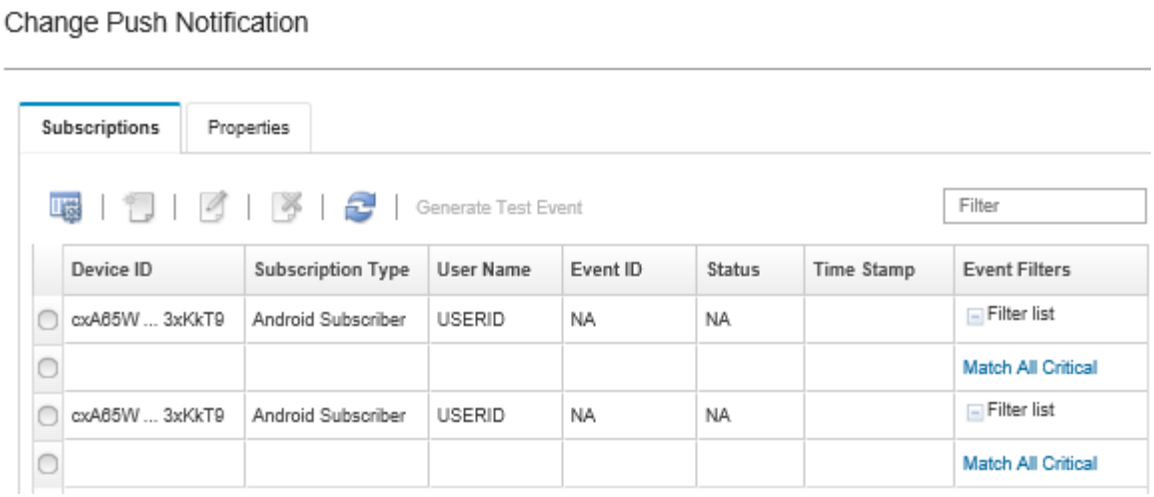
- È possibile modificare le proprietà del servizio di notifica del dispositivo dalla scheda **Servizio push** nella pagina Inoltro eventi facendo clic sul collegamento relativo al servizio di notifica push (Google o Apple) nella colonna **Nome** per visualizzare la finestra di dialogo Modifica notifica push, quindi fare clic sulla scheda **Proprietà**.



- È possibile abilitare e disabilitare le sottoscrizioni:
  - Abilitare o disabilitare tutte le sottoscrizioni per un servizio di notifica di un dispositivo specifico dalla scheda **Servizio push** nella pagina Inoltro eventi selezionando lo stato **ATTIVATO** o **DISATTIVATO** nella tabella del servizio di notifica del dispositivo.
  - Abilitare o disabilitare tutte le sottoscrizioni per uno specifico dispositivo dall'app Lenovo XClarity Mobile toccando **Impostazioni → Notifica push**, quindi abilitando o disabilitando l'opzione Notifica push abilitata.
  - Abilitare o disabilitare una sottoscrizione specifica dall'app Lenovo XClarity Mobile toccando **Impostazioni → Notifica push**, toccando una connessione Lenovo XClarity Administrator e abilitando almeno un filtro eventi oppure disabilitando tutti i filtri eventi.
- È possibile generare un evento di prova per tutte le sottoscrizioni per uno specifico servizio mobile dalla scheda **Servizio push** nella pagina Inoltro eventi selezionando il servizio mobile e facendo clic su **Genera evento di test**.
- È possibile visualizzare un elenco delle sottoscrizioni correnti. Dalla scheda **Servizio push** nella pagina Inoltro eventi, fare clic sul collegamento del servizio di notifica del dispositivo applicabile (Android o iOS) nella colonna **Nome** per visualizzare la finestra di dialogo Modifica notifica push, quindi fare clic sulla scheda **Sottoscrizioni**. L'ID del dispositivo identifica ciascuna sottoscrizione.

  Suggerimenti:

  - L'ID del dispositivo è costituito dalla prima cifra e dalle ultime 6 cifre dell'ID della registrazione push. L'ID della registrazione push può essere individuato dall'app Lenovo XClarity Mobile toccando **Impostazioni → Informazioni su → ID registrazione push**.
  - Se l'utente ha eseguito il login con uno dei seguenti ruoli vengono visualizzate tutte le sottoscrizioni; altrimenti vengono visualizzate solo le sottoscrizioni per l'utente che ha eseguito il login.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- È possibile visualizzare l'elenco dei filtri eventi assegnati alla sottoscrizione dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push espandendo l'opzione **Elenco filtri** nella colonna **Filtri eventi** per la sottoscrizione.



- È possibile creare i filtri eventi per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic sull'icona **Crea** ( ).

Nota: questi filtri eventi si applicano solo a una sottoscrizione specifica e non possono essere utilizzati da altre sottoscrizioni.

È inoltre possibile modificare o rimuovere un filtro eventi selezionando il filtro eventi e facendo clic rispettivamente sull'icona **Modifica** ( ) o **Rimuovi** ( ).

- È possibile determinare lo stato dell'esecuzione del push più recente per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push. La colonna **Timestamp** indica la data e l'ora dell'ultimo push. L'opzione **Stato** indica se la notifica push è stata recapitata correttamente al servizio push. Non esiste nessuno stato indicante se la notifica push è stata correttamente recapitata dal servizio al dispositivo. Se il recapito di un servizio push non riesce, la colonna Stato fornisce informazioni aggiuntive relative all'errore.
- È possibile generare un evento di prova per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic su **Genera evento di test**.
- È possibile rimuovere una sottoscrizione dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic sull'icona **Rimuovi** ( ).

Inoltro di eventi ai servizi WebSocket

È possibile configurare Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi ai servizi WebSocket.

Informazioni su questa attività

Le sottoscrizioni WebSocket non vengono memorizzate in modo permanente in Lenovo XClarity Administrator. Quando Lenovo XClarity Administrator viene riavviato, i sottoscrittori WebSocket devono eseguire nuovamente la registrazione.

Procedura

Per eseguire il push della notifica dell'evento a un servizio WebSocket, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Servizi push**.

Passo 3. Fare clic sul collegamento per il **servizio WebSocket** nella colonna **Nome**. Viene visualizzata la finestra di dialogo Modifica notifica push.

Passo 4. Fare clic sulla scheda **Sottoscrizioni**.

Passo 5. Fare clic sull'icona **Crea** ( ).

Passo 6. Immettere l'indirizzo IP dell'host di destinazione.

Passo 7. Fare clic su **Crea**.

Passo 8. Selezionare la nuova sottoscrizione, fare clic su **Genera evento di test**, quindi verificare che gli eventi siano inoltrati correttamente al servizio WebSocket.

Risultati

Dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push, è possibile eseguire le seguenti azioni su una sottoscrizione WebSocket selezionata:

- Aggiornare l'elenco dei servizi WebSocket facendo clic sull'icona **Aggiorna** ( ).
- Eliminare le sottoscrizioni selezionando le sottoscrizioni e facendo clic sull'icona **Elimina** ( ).

- Determinare lo stato dell'ultimo push tentato per una sottoscrizione specifica visualizzando il contenuto della colonna **Stato**. Se il tentativo non riesce, questa colonna contiene un messaggio che descrive l'errore.

Dalla scheda **Proprietà** nella finestra di dialogo Modifica notifica push, procedere come segue:

- Modificare le proprietà del servizio WebSocket, tra cui il tempo di inattività della connessione, le dimensioni massime del buffer, il numero massimo di sottoscrittori e il periodo di timeout del registro.
- È possibile ripristinare i valori predefiniti del servizio WebSocket facendo clic su **Ripristina valori predefiniti**.
- Sospendere l'esecuzione del push delle notifiche degli eventi a tutte le sottoscrizioni per il servizio WebSocket impostando l'opzione **Stato** su Disattivato.

Dalla scheda **Servizio push** nella pagina Inoltro eventi, è possibile generare un evento di prova per tutte le sottoscrizioni WebSocket selezionando il servizio WebSocket e facendo clic su **Genera evento di test**.

Creazione di filtri eventi per dispositivi mobili e WebSockets

È possibile creare filtri eventi globali da utilizzare in una o più sottoscrizioni per dispositivi mobili e WebSockets. È inoltre possibile creare filtri eventi univoci per una sottoscrizione.

Prima di iniziare

È necessario disporre dei privilegi di supervisore per creare i filtri eventi.

È possibile creare un massimo di 20 filtri eventi globali.

Informazioni su questa attività

Sono predefiniti i seguenti filtri eventi globali:

- **Associa tutti gli eventi Critico**. Questo filtro associa tutti gli eventi critici generati dal dispositivo gestito o da XClarity Administrator.
- **Associa tutti gli eventi Avvertenza**. Questo filtro associa tutti gli eventi di avvertenza generati dal dispositivo gestito o da XClarity Administrator.

Procedura

Per creare un filtro eventi globale, completare le seguenti operazioni.

- Creare un filtro eventi globale da utilizzare per ciascuna sottoscrizione.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.
  2. Fare clic sulla scheda **Filtri push**.
  3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo filtro push.
  4. Specificare il nome e la descrizione dell'opzione per questo filtro eventi.
  5. Fare clic su **Avanti** per visualizzare la scheda **Sistemi**.
  6. Selezionare i dispositivi che si desidera monitorare.

     Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna

UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

7. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.
8. Selezionare i componenti e le gravità per cui si desidera inoltrare gli eventi.

   Suggerimento:
   - Per inoltrare tutti gli eventi hardware, selezionare **Associa tutti gli eventi**.
   - Per inoltrare gli eventi di controllo, selezionare **Includi tutti gli eventi di controllo**.
   - Per inoltrare gli eventi di garanzia, selezionare **Includi eventi garanzia**.
9. Fare clic su **Crea**.

- Creare un filtro eventi per una sottoscrizione specifica:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro nuovi eventi.
  2. Fare clic sulla scheda **Filtri push**.
  3. Selezionare il collegamento per il tipo di dispositivo mobile (Android o iOS) nella colonna Nome della tabella. Viene visualizzata la finestra di dialogo Modifica notifica push.
  4. Fare clic sulla scheda **Sottoscrizioni** per visualizzare un elenco di sottoscrizioni attive.
  5. Selezionare la sottoscrizione e fare clic sull'icona **Crea** (). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo filtro eventi.
  6. Specificare il nome e la descrizione dell'opzione per questo filtro eventi.
  7. Fare clic su **Avanti** per visualizzare la scheda **Sistemi**.
  8. Selezionare i dispositivi che si desidera monitorare.

     Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.
  9. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.
  10. Selezionare i componenti e le gravità per cui si desidera inoltrare gli eventi.

      Suggerimento:
      - Per inoltrare tutti gli eventi hardware, selezionare **Associa tutti gli eventi**.
      - Per inoltrare gli eventi di controllo, selezionare **Includi tutti gli eventi di controllo**.
      - Per inoltrare gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  11. Fare clic su **Crea**.

Al termine

Dalla scheda Filtri push nella pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un filtro eventi selezionato:

- Aggiornare l'elenco dei filtri eventi facendo clic sull'icona **Aggiorna** ().
- Visualizzare i dettagli su un filtro eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del filtro eventi e filtrare i criteri facendo clic sull'icona **Modifica** ().

Eliminare il filtro eventi facendo clic sull'icona **Elimina** ( ).

Utilizzo dei processi

I *processi* sono attività che richiedono tempi di esecuzione superiori per uno o più dispositivi. È possibile pianificare l'esecuzione di determinati processi per una sola volta (immediatamente o in secondo momento), in modo periodico o quando si verifica un evento specifico.

I processi vengono eseguiti in background. È possibile visualizzare lo stato di ciascun processo dal log dei processi.

Monitoraggio dei processi

È possibile visualizzare un log di tutti i processi avviati da Lenovo XClarity Administrator. Il log dei processi include i processi in esecuzione, completati o in errore.

Informazioni su questa attività

I *processi* sono attività che richiedono tempi di esecuzione superiori per uno o più dispositivi. Ad esempio, se un sistema operativo viene distribuito su più server, ciascuna distribuzione server viene elencata come processo separato.

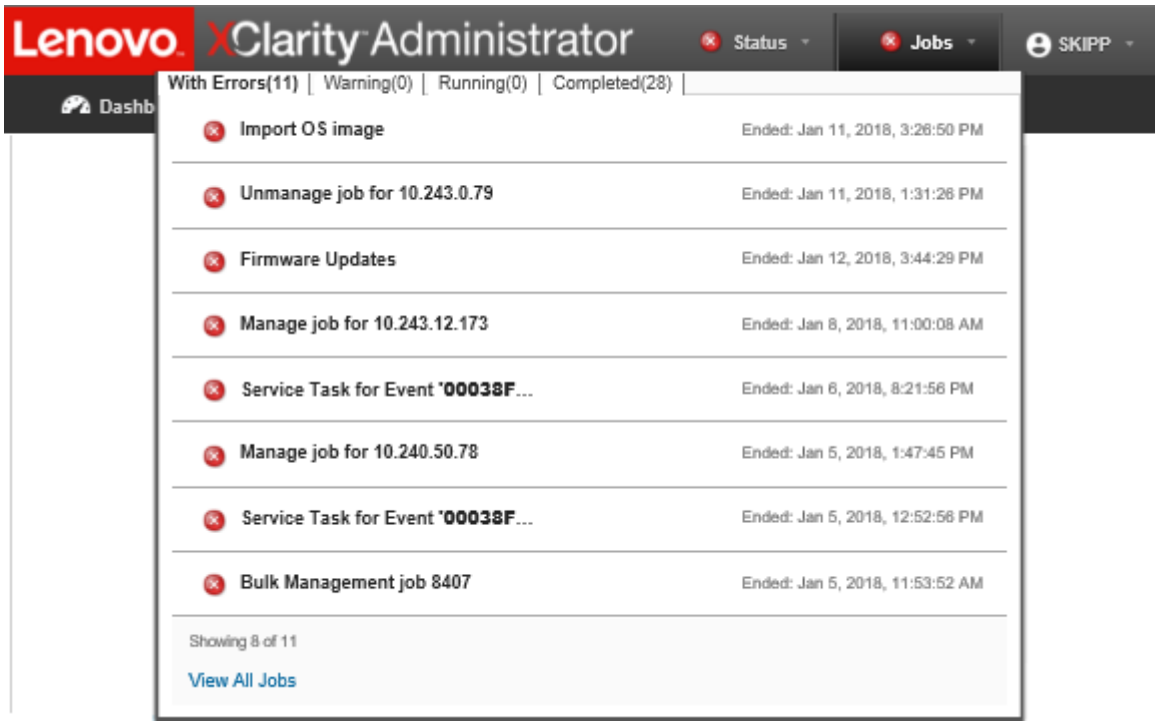
I processi vengono eseguiti in background. È possibile visualizzare lo stato di ciascun processo dal log dei processi.

Il log dei processi contiene informazioni su ciascun processo. Il log può contenere massimo 1.000 processi o 1 GB. Quando le dimensioni massime vengono raggiunte, i processi meno recenti completati correttamente vengono eliminati. Se nel log non sono presenti processi completati correttamente, vengono eliminati i processi meno recenti completati con avvisi. Se nel log non sono presenti processi completati correttamente o con avvisi, vengono eliminati i processi meno recenti completati con errori.

Procedura

Completare una delle seguenti operazioni per visualizzare il log processi.

- Dalla barra del titolo XClarity Administrator, fare clic su **Processi** per visualizzare un riepilogo dei processi in esecuzione, completati e in errore.



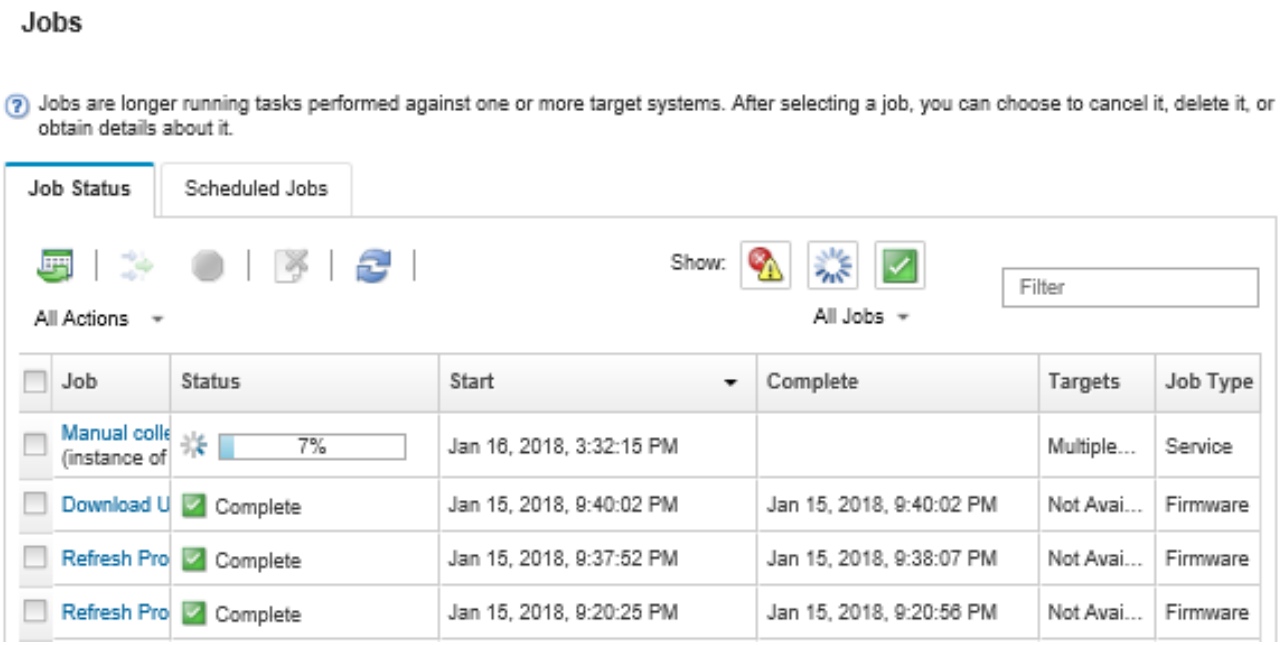
Da questo menu a discesa è possibile fare clic sulle seguenti schede:
- **Errori**. Visualizza un elenco di tutti i processi con errori associati.
- **Avvisi**. Visualizza un elenco di tutti i processi con avvisi associati.
- **Esecuzione in corso**. Visualizza un elenco di tutti i processi attualmente in esecuzione.
- **Completato**. Visualizza un elenco di tutti i processi completati.

Passare con il mouse sulla voce relativa a un processo nel menu a discesa per ulteriori informazioni relative al processo, quali lo stato, l'avanzamento e l'utente che ha creato il processo.

- Dalla barra del titolo di XClarity Administrator, fare clic su **Processi** e sul collegamento **Visualizza tutti i processi** per visualizzare la pagina Stato dei processi.
- Dalla barra dei menu di XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Stato dei processi** per visualizzare la pagina Stato dei processi.

Al termine

Viene visualizzata la pagina Processi con un elenco di tutti i processi per XClarity Administrator.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Per creare pianificazioni dei processi, fare clic sulla scheda **Processi pianificati** (vedere Pianificazione dei processi).
- Visualizzare più informazioni su un processo, facendo clic sulla descrizione del processo nella colonna **Processi**. Viene visualizzata una finestra di dialogo con un elenco di attività secondarie (processi secondari) e le relative destinazioni, un riepilogo delle attività secondarie, incluse eventuali azioni necessarie e i dettagli del log, come la gravità e il timestamp per ogni messaggio. È possibile scegliere di visualizzare o nascondere i log per le attività secondarie.
- Per i processi pianificati, è possibile visualizzare le informazioni sulla pianificazione del processo facendo clic su "questo" collegamento, sotto la descrizione del processo nella colonna **Processi**.
- Modificare il numero di processi visualizzati per pagina. L'impostazione predefinita è 10 processi. È possibile visualizzare 25, 50 o tutti i processi.
- Restringere l'elenco dei processi visualizzati:
  - Per elencare solo i processi di una fonte specifica, fare clic su **Tipi di processo** e scegliere tra le seguenti opzioni.
    - **Tutti i tipi di processo**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Accesso remoto**
    - **ID sistema**
    - **Immagini sistema operativo**
    - **Distribuzione sistema operativo**
    - **Esportazione profilo sistema operativo**
    - **Custom**
    - **Inventory**
    - **Sconosciuto**

  - Per elencare solo i processi pianificati, associati a un tipo specifico di pianificazione, fare clic su **Tipi di pianificazione** e scegliere tra le seguenti opzioni.
    - **Tutti i tipi di pianificazione**
    - **Una volta**
    - **Periodico**
    - **Attivato**
  - Nascondere o mostrare i processi con errori o avvertenze facendo clic sull'icona **Nascondi processi con errori/avvisi** ( ).
  - Nascondere o mostrare i processi attualmente in esecuzione facendo clic sull'icona **Nascondi processi in esecuzione** ( ).
  - Nascondere o mostrare i processi completati facendo clic sull'icona **Nascondi processi completati** ( ).
  - Elencare solo i processi che contengono testo specifico immettendo il testo nel campo **Filtro**.
  - Se il filtro viene applicato alla pagina, rimuovere il filtro facendo clic sull'icona **Mostra tutti i processi** ( ).
  - Ordinare i processi per colonna facendo clic su un'intestazione di colonna.
- Esportare l'elenco dei processi come file CSV facendo clic sull'icona **Esporta come CSV** ( ).

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Annullare i processi o le sottoattività in esecuzione selezionando uno o più processi in esecuzione e facendo clic sull'icona **Interrompi** ( ).

  Nota: l'annullamento del processo potrebbe richiedere alcuni minuti.
- Eliminare i processi o le sottoattività completati dal log dei processi selezionando uno o più processi o sottoattività completati e facendo clic sull'icona **Elimina** ( ).
- Esportare le informazioni su processi specifici selezionando i processi e facendo clic sull'icona **Esporta come CSV** ( ).
- Aggiornare il log dei processi facendo clic sull'icona **Aggiorna** ( ).

Pianificazione dei processi

È possibile creare pianificazioni in Lenovo XClarity Administrator per eseguire determinate attività in momenti specifici.

Informazioni su questa attività

È possibile pianificare i seguenti tipi di processi:
- Attività semplici, come spegnimento e riavvio
- Raccolta dei dati di servizio per dispositivi specifici
- Aggiornamento dei cataloghi degli aggiornamenti firmware e dei driver di dispositivo del sistema operativo dal sito Web Lenovo
- Aggiornando XClarity Administrator viene aggiornato il catalogo dal sito Web Lenovo
- Download di firmware dal sito Web Lenovo
- Aggiornamento del firmware e dei driver di dispositivo del sistema operativo sui dispositivi gestiti
- Backup dei dati e delle impostazioni di XClarity Administrator
- Backup e ripristino dei dati di configurazione di uno switch

È possibile pianificare l'esecuzione dei processi:
- Una volta (immediatamente o in un secondo momento)
- Periodico
- Quando si verifica un evento specifico

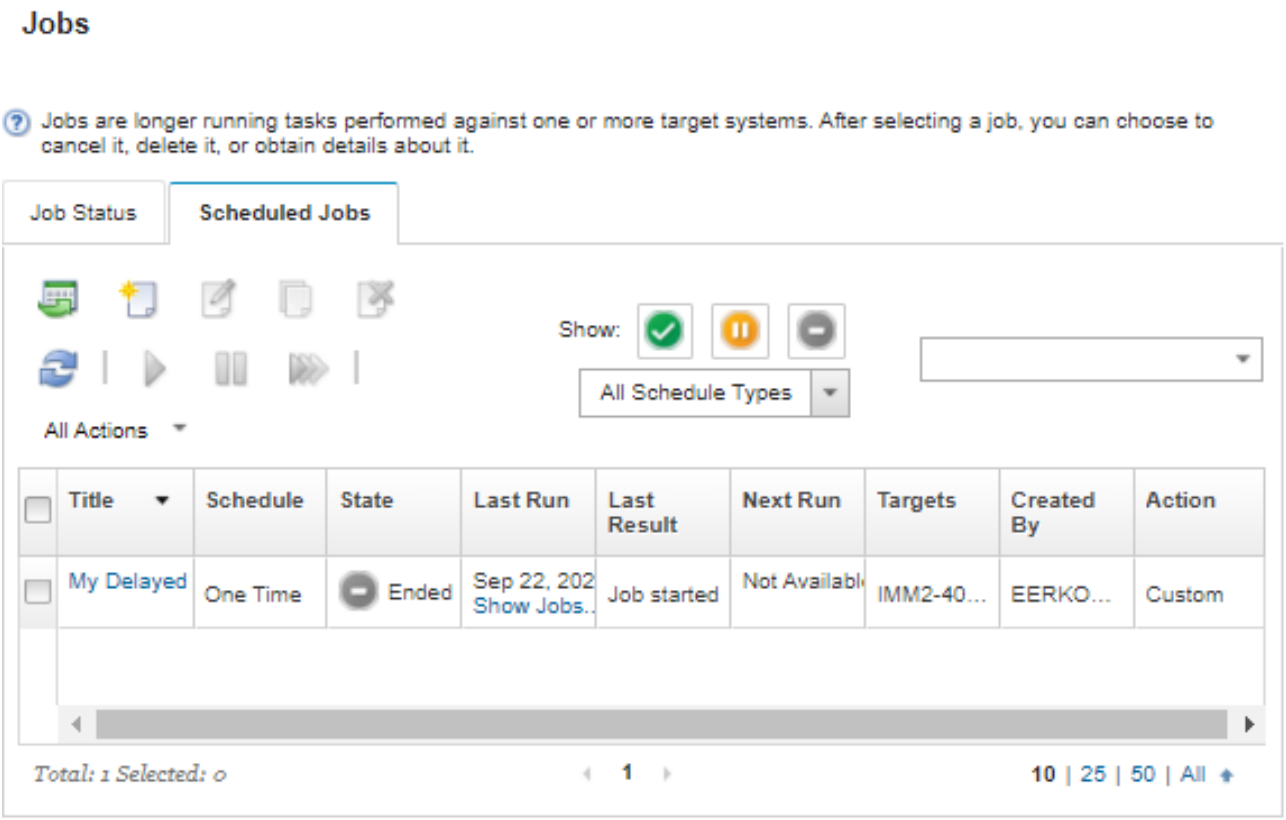
Procedura

Per creare e pianificare un processo, attenersi alla procedura descritta di seguito.

- Per le attività complesse, come l'aggiornamento del firmware e la raccolta dei dati di servizio, creare il processo dalla finestra di dialogo o dalla pagina dell'attività corrente.
  1. Fare clic su **Pianificazione** per creare una pianificazione per l'esecuzione di questa attività. Viene visualizzata la finestra di dialogo Pianifica nuovo processo.
  2. Immettere il nome del processo.
  3. Specificare quando eseguire il processo. Le opzioni disponibili variano a seconda del tipo di processo. Alcuni processi non possono essere periodici o attivati da un evento
     - **Una volta**. Questi processi vengono eseguiti solo una volta. Specificare la data e l'ora in cui si desidera eseguire questo processo.
     - **Periodico**. Questi processi vengono eseguiti più di una volta. Specificare quando e con che frequenza si desidera eseguire questo processo.
     - **Attivato da evento**. Questi processi vengono eseguiti quando si verifica un evento specifico.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare l'evento che attiva il processo.
  4. Fare clic su **Crea processo**.
- Per attività semplici, come l'accensione e il riavvio del sistema, creare la pianificazione del processo dalla pagina "Processi".
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Processo pianificato** per visualizzare la pagina "Processi pianificati".
  2. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Pianifica nuovi processi".
  3. Immettere il nome del processo.
  4. Specificare quando eseguire il processo.
     - **Una volta**. Questi processi vengono eseguiti solo una volta.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo.
     - **Periodico**. Questi processi vengono eseguiti più di una volta.
       a. Specificare quando e con che frequenza si desidera eseguire questo processo.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo**.**
     - **Attivato da evento**. Questi processi vengono eseguiti quando si verifica un evento specifico.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo e fare clic su **Avanti**.
       c. Selezionare l'evento che attiva il processo.
  5. Fare clic su **Crea**.

Al termine

Viene visualizzata la scheda Processi pianificati con un elenco di tutte le pianificazioni dei processi in XClarity Administrator.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Per visualizzare le informazioni su tutti i processi attivi e completati per una specifica pianificazione di un processo, fare clic sul collegamento nella colonna **Processo**.
  - Per restringere l'elenco di pianificazioni dei processi visualizzati per un tipo specifico di pianificazione, fare clic su **Tipi di pianificazione** e scegliere tra le seguenti opzioni:
    - **Tutti i tipi di pianificazione**
    - **Una volta**
    - **Periodico**
    - **Attivato**
  - Per nascondere o mostrare solo le pianificazioni dei processi che si trovano in uno stato specifico, fare clic su una delle seguenti icone:
    - Per visualizzare tutti i processi pianificati attivi, fare clic sull'icona **Attivo** icona ( ).
    - Per visualizzare tutti i processi pianificati non attivi, fare clic sull'icona **In pausa** icona ( ).
    - Per visualizzare tutti i processi pianificati già eseguiti, di cui non è stata pianificata una nuova esecuzione, fare clic sull'icona **Terminato** ( ).
  - Elencare solo i processi pianificati che contengono testo specifico immettendo il testo nel campo **Filtro**.
  - Ordinare i processi pianificati per colonna facendo clic su un'intestazione di colonna.
- Per visualizzare l'ultima esecuzione del processo, controllare la colonna **Ultima esecuzione**. Per visualizzare lo stato dell'ultima esecuzione del processo, fare clic sul collegamento "Stato del processo" in questa colonna.

- Per visualizzare quando è pianificata la prossima esecuzione del processo, controllare la colonna **Prossima esecuzione**. Per visualizzare un elenco di tutte le date e gli orari futuri, fare clic sul collegamento "Altro" in questa colonna.
- Per eseguire immediatamente il processo associato alla pianificazione, fare clic sull'icona **Esegui** ( ).
- Per disabilitare o abilitare la pianificazione di un processo, fare clic rispettivamente sull'icona **Pausa** ( ) o sull'icona **Attiva** ( ).
- Per copiare e modificare la pianificazione di un processo, fare clic sull'icona **Copia** ( ).
- Per modificare la pianificazione di un processo, fare clic sull'icona **Modifica** ( ).
- Per eliminare uno o più pianificazioni del processo selezionato, fare clic sull'icona **Elimina** ( ).
- Esportare le informazioni sulle pianificazioni di processi specifici selezionando le pianificazioni e facendo clic sull'icona **Esporta come CSV** ( ).
- Per aggiornare l'elenco delle pianificazione dei processi, fare clic su **Tutte le azioni → Aggiorna**.

Aggiunta di una risoluzione e di commenti a un processo

È possibile aggiungere una risoluzione e i commenti a un processo completato, indipendentemente dallo stato di errore o di riuscita. È possibile eseguire questa operazione per un processo principale e per le attività secondarie del processo.

Procedura

Effettuare una delle seguenti operazioni per aggiungere una risoluzione e i commenti a un processo.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Stato dei processi** per visualizzare la pagina Stato dei processi.

Passo 2. Fare clic sul collegamento per il processo nella colonna **Processo** per visualizzare i dettagli del processo.

Passo 3. Fare clic sull'icona **Note** ( ) per visualizzare la finestra di dialogo Note.

Da questa finestra di dialogo, è possibile visualizzare una cronologia di tutte le note e le risoluzioni aggiunte al processo. È possibile cancellare la cronologia facendo clic su **Cancella tutti i record**.

Passo 4. Scegliere una delle seguenti risoluzioni.
- **Nessuna modifica**
- **Analisi in corso**
- **Risolto**
- **Interrotto**

Passo 5. Aggiungere una nota nel campo **Nota**.

Passo 6. Fare clic su **Applica**.

Nella pagina Stato dei processi, La risoluzione viene visualizzata nella colonna **Stato** di questo processo.

Capitolo 3. Utilizzo di assistenza e supporto

L'interfaccia Web di Lenovo XClarity Administrator fornisce un set di strumenti che è possibile utilizzare per definire i contatti di supporto per ciascun dispositivo gestito, raccogliere e inviare file di servizio a Supporto Lenovo, configurare notifiche automatiche per i fornitori di servizi quando si verifica un evento che richiede assistenza per specifici dispositivi e visualizzare il ticket di assistenza e le informazioni sulla garanzia. È possibile contattare Supporto Lenovo per ottenere indicazioni e assistenza tecnica quando si riscontrano problemi.

Ulteriori informazioni: XClarity Administrator: assistenza e supporto

Ottenere i comunicati da Lenovo

Lenovo aggiorna costantemente il sito Web di supporto con annunci, avvisi di sicurezza e impatto sui servizi online. È possibile consentire a Lenovo di inviare questi annunci come comunicati nell'interfaccia Web di Lenovo XClarity Administrator.

Prima di iniziare

XClarity Administrator deve avere accesso a Internet per ricevere gli annunci da Lenovo.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti dai comunicati.

Informazioni su questa attività

La ricezione dei comunicati è abilitata per impostazione predefinita.

Se abilitata, Lenovo invia i seguenti tipi di comunicati.
- Disponibilità di nuove versioni o firmware di XClarity Administrator
- Avvisi di sicurezza, come vulnerabilità rilevate che interessano firmware o server di gestione
- Interruzioni pianificate che hanno un impatto sui servizi online Lenovo XClarity

È possibile visualizzare i comunicati in vari modi.

- I nuovi comunicati vengono visualizzati in messaggi popup nell'interfaccia Web di XClarity Administrator.
- È possibile visualizzare un elenco dei comunicati di servizio degli ultimi 30 giorni dalla pagina Login facendo clic sul menu azioni utente (

) e selezionando **Servizio comunicati Lenovo**.
- È possibile configurare un server d'inoltro delle e-mail che abilita l'opzione **Includi eventi dei comunicati** per inviare i comunicati all'indirizzo e-mail (vedere Configurazione dell'inoltro degli eventi a un servizio di posta elettronica mediante il protocollo SMTP nella documentazione online di XClarity Administrator).

Procedura

Completare la procedura seguente per abilitare la ricezione dei comunicati.

Passo 1. Sulla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**, quindi su **Servizio comunicati Lenovo** nel riquadro di navigazione sinistro per visualizzare la pagina Servizio comunicato Lenovo.

Passo 2. Selezionare **Accetto di ricevere i comunicati da Lenovo**.

Passo 3. Fare clic su **Applica**.

© Copyright Lenovo 2015, 2025

Visualizzazione delle informazioni sulla garanzia

È possibile determinare lo stato di garanzia (incluse le garanzie estese) dei dispositivi gestiti.

Prima di iniziare

Lenovo XClarity Administrator deve disporre dell'accesso ai seguenti URL per raccogliere le informazioni di garanzia per i dispositivi gestiti. Verificare che l'accesso a questi URL non sia bloccato da firewall. Per ulteriori informazioni, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

- Database Lenovo Warranty (tutti i paesi) - https://ibase.lenovo.com/POIRequest.aspx
- Database Lenovo Warranty (solo Cina) - http://service.lenovo.com.cn:83/webservice/NewProductQueryService.asmx
- Servizio Web Lenovo Warranty - http://supportapi.lenovo.com/warranty/ o https://supportapi.lenovo.com/warranty/

È possibile abilitare o disabilitare questi URL relativi alla garanzia in XClarity Administrator facendo clic su **Tutte le azioni → Configura collegamenti garanzia**.

Nota: Per i dispositivi RackSwitch, la colonna **Numero di serie** mostra il numero di serie autorizzato.

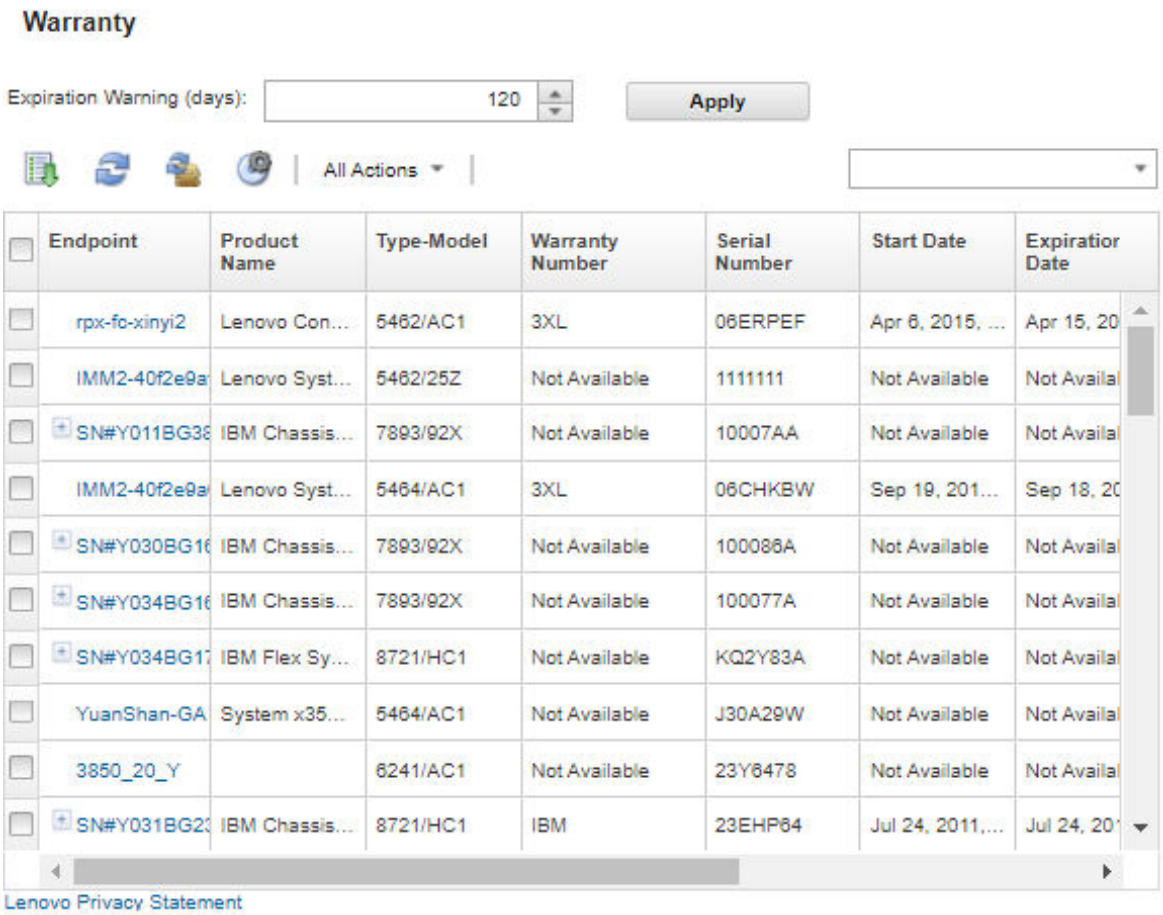
Procedura

Per visualizzare lo stato della garanzia dei dispositivi gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.

Passo 2. Fare clic su **Garanzia** nel riquadro di navigazione sinistro per visualizzare la pagina Garanzia.

Questa pagina contiene una tabella contenente le informazioni sulla garanzia (tra cui data di inizio, data di fine e stato) per ogni dispositivo gestito.



Al termine

Dalla pagina Garanzia è possibile completare le seguenti azioni:

- Impostare quando si desidera essere avvisati sulla scadenza della garanzia per un dispositivo gestito mediante il campo **Avviso scadenza**. Il valore predefinito è 30 giorni prima della scadenza della garanzia.
- Consultare le informazioni sulla garanzia (se disponibili) per uno specifico dispositivo sul sito Web del supporto Lenovo facendo clic sul collegamento nella colonna **Stato**.
- Esportare lo stato di garanzia per tutti i dispositivi gestiti in un file CSV facendo clic sull'icona **Scarica CSV** ( ).
- Aggiornare le informazioni di garanzia per tutti i dispositivi gestiti facendo clic sull'icona **Aggiorna elenco server** ( ).

Configurazione dell'invio di notifiche automatiche dei problemi

È possibile creare un server d'inoltro di servizio per inviare automaticamente i dati di servizio al fornitore di servizi preferito quando si verifica un evento che richiede assistenza su specifici dispositivi gestiti. È possibile inviare i dati di servizio per il dispositivo a Supporto Lenovo (Call Home), al tecnico dell'assistenza Lenovo mediante la funzione Caricamento Lenovo oppure a un altro fornitore di servizi mediante SFTP.

È possibile creare e abilitare fino a 50 server d'inoltro di servizio totali per Call Home, Funzione Caricamento Lenovo o SFTP.

Configurazione dell'invio di notifiche automatiche dei problemi al supporto Lenovo (Call Home)

È possibile creare un server d'inoltro di servizio in grado di inviare automaticamente dati di servizio per un dispositivo gestito a Supporto Lenovo mediante Call Home, quando determinati eventi di manutenzione, come una memoria irrecuperabile, vengono ricevuti da specifici dispositivi gestiti, affinché il problema possa essere risolto. Il servizio inoltrato viene denominato "Call Home predefinito".

Lenovo è impegnata nella sicurezza. Se abilitata, Call Home invia i dati di servizio alla funzione Caricamento Lenovo quando un dispositivo riporta un guasto hardware o quando si sceglie di avviare una Call Home manuale. I dati di servizio che vengono in genere caricati manualmente sul supporto Lenovo vengono automaticamente inviati alla Funzione Caricamento Lenovo su HTTPS mediante TLS 1.2 o versione successiva. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nella Funzione Caricamento Lenovo è limitato al personale di assistenza autorizzato.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Accertarsi che tutte le porte richieste da Lenovo XClarity Administrator (incluse le porte richieste per Call Home) siano disponibili prima di abilitare Call Home. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Una volta configurato Call Home, il server d'inoltro di servizio **Lenovo Call Home predefinito** viene aggiunto alla pagina Server d'inoltro di servizio. È possibile modificare questo server d'inoltro di servizio per configurare impostazioni aggiuntive, quali i dispositivi associati a questo server d'inoltro di servizio. Tutti i dispositivi vengono associati per impostazione predefinita.

Attenzione: Se l'opzione **Associa tutti i dispositivi** è disabilitata, i dispositivi non selezionati in modo esplicito, singolarmente o tramite gruppi di risorse, in un server d'inoltro Call Home abilitato *non* avvieranno una Call Home per il supporto Lenovo per gli eventi che richiedono assistenza.

Attualmente non è disponibile l'opzione Call Home di esclusione per dispositivi specifici. Nella remota situazione in cui si desidera disporre di un sottoinsieme di dispositivi non Call Home per eventi che richiedono assistenza, è possibile creare una serie di gruppi di risorse statici e dinamici che evitino i dispositivi desiderati e quindi aggiungere questi gruppi di risorse al server d'inoltro Call Home.

Attenzione: Se l'opzione **Associa tutti i dispositivi** non è abilitata per i server d'inoltro Call Home, Call Home non viene avviata per alcun dispositivo. Per questo motivo, si consiglia di disporre di almeno un server d'inoltro Call Home con l'opzione **Associa tutti i dispositivi** abilitata come server d'inoltro di ultima istanza.

Importante:

- Quando si abilita un server d'inoltro di servizio Call Home in Lenovo XClarity Administrator, Call Home è disabilitata in ogni dispositivo gestito, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi o si intende disabilitare Call Home in XClarity Administrator, è possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator

anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento. Per informazioni su come riabilitare Call Home su tutti i dispositivi gestiti quando il server d'inoltro di servizio per Call Home è disabilitato, vedere Riabilitazione di Call Home su tutti i dispositivi gestiti.

- Sebbene XClarity Administrator supporti la funzionalità Call Home per i dispositivi ThinkAgile e ThinkSystem, il controller di gestione della scheda di base per alcuni dispositivi ThinkAgile e ThinkSystem non include il supporto Call Home. Pertanto, non è possibile abilitare o disabilitare Call Home su questi dispositivi. Call Home può essere abilitato solo per i dispositivi al livello di XClarity Administrator.

Informazioni su questa attività

Un *server d'inoltro di servizio* definisce le informazioni sulla destinazione dell'invio dei file di dati di servizio quando si verifica un evento che richiede assistenza. È possibile definire fino a 50 server d'inoltro di servizio.

- **Se un server d'inoltro di servizio Call Home non è configurato**, è possibile aprire manualmente un ticket di assistenza e inviare file di servizio a Centro assistenza clienti Lenovo seguendo le istruzioni fornite nel Pagina Web per la richiesta di un nuovo servizio. Per informazioni sulla raccolta e sul download di file di servizio, vedere Raccolta e download dei file di servizio Lenovo XClarity Administrator, Raccolta e download dei dati di servizio per un dispositivo.
- **Se un server d'inoltro di servizio Call Home è configurato ma non abilitato**, è possibile aprire *manualmente* un ticket di assistenza mediante la funzione Call Home per raccogliere e trasferire file di servizio al Centro assistenza clienti Lenovo in qualsiasi momento. Per ulteriori informazioni, vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo.
- **Se un server d'inoltro di Call Home è configurato e abilitato**, XClarity Administrator apre *automaticamente* un ticket di assistenza, raccoglie i dati di servizio, li salva in un file di archivio e trasferisce il file di archivio del servizio a Funzione Caricamento Lenovo quando si verifica un evento che richiede assistenza perché il problema venga risolto. Il file di archivio del servizio contiene i dati di servizio per il dispositivo e per XClarity Administrator.

  Nota: Per i Server ThinkSystem V3 e V4 (con XCC2 o XCC3), XClarity Administrator salva i dati di servizio in due file nel repository.

  - **File di servizio**. (.zip) Questo file contiene informazioni sull'assistenza del dispositivo e l'inventario in un formato facilmente leggibile. Questo file viene inviato automaticamente alla Funzione Caricamento Lenovo quando si verifica un evento di manutenzione.
  - **File di debug**. (.tzz) Il file contiene tutte le informazioni sull'assistenza del dispositivo, l'inventario e i log di debug che verranno utilizzati da Funzione Caricamento Lenovo. È possibile inviare manualmente questo file al supporto Lenovo, se sono necessarie ulteriori informazioni per risolvere un problema.

  Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui XClarity Administrator e le informazioni sull'assistenza, l'inventario e i log di debug) in un singolo file di servizio nel repository. Questo file viene inviato al Centro assistenza clienti Lenovo quando si verifica un evento di manutenzione.

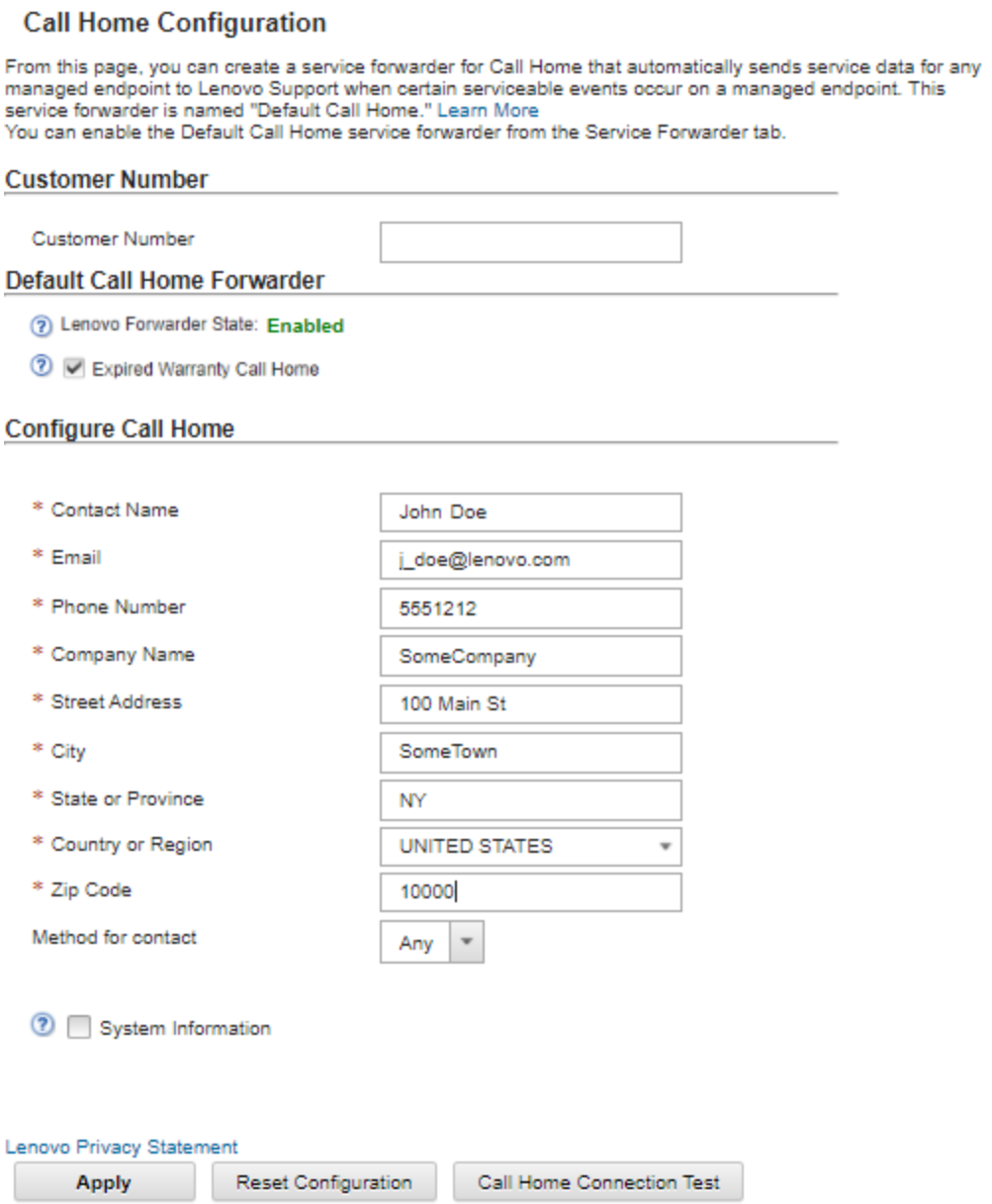
  Call Home viene eliminato per gli eventi ripetuti per qualsiasi dispositivo, se un ticket di assistenza è aperto per quell'evento su quel dispositivo. Call Home viene eliminato anche per gli eventi simili di qualsiasi dispositivo ThinkAgile e ThinkSystem, se un ticket di assistenza è aperto per un evento su quel dispositivo. Gli eventi ThinkAgile e ThinkSystem sono stringhe di 16 caratteri nel seguente formato *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (ad esempio, `806F010D0401FFFF`). Gli eventi sono simili se hanno lo stesso tipo di lettura, tipo di sensore e ID entità. Ad esempio, se un ticket di assistenza è aperto per l'evento 806F010D0401FFFF su uno specifico dispositivo ThinkAgile o ThinkSystem, tutti gli eventi che si verificano su tale dispositivo con ID evento del tipo *xx*`6F01`*xx*`04`*xxxxxx*, dove *x* è un qualsiasi carattere alfanumerico, vengono eliminati.

  Per informazioni sulla visualizzazione dei ticket di assistenza aperti automaticamente da un server d'inoltro di servizio Call Home, vedere Visualizzazione di ticket di assistenza e stato.

Procedura

Completare le seguenti operazioni per configurare un servizio inviato per Call Home.

- Configurare Call Home per tutti i dispositivi gestiti (correnti e futuri):
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.
  2. Fare clic su **Configurazione Call Home** nel riquadro di navigazione sinistro per visualizzare la pagina Configurazione Call Home.



  3. (Facoltativo) Specificare il numero cliente Lenovo predefinito da utilizzare quando si segnalano i problemi con XClarity Administrator.

     Suggerimento: il numero cliente è indicato nell'e-mail di abilitazione ricevuta al momento dell'acquisto di Lenovo XClarity Pro.

4. Deselezionare **Call Home garanzia scaduta** per impedire l'apertura automatica dei ticket di assistenza da parte di Call Home per i dispositivi con garanzie scadute (facoltativo).

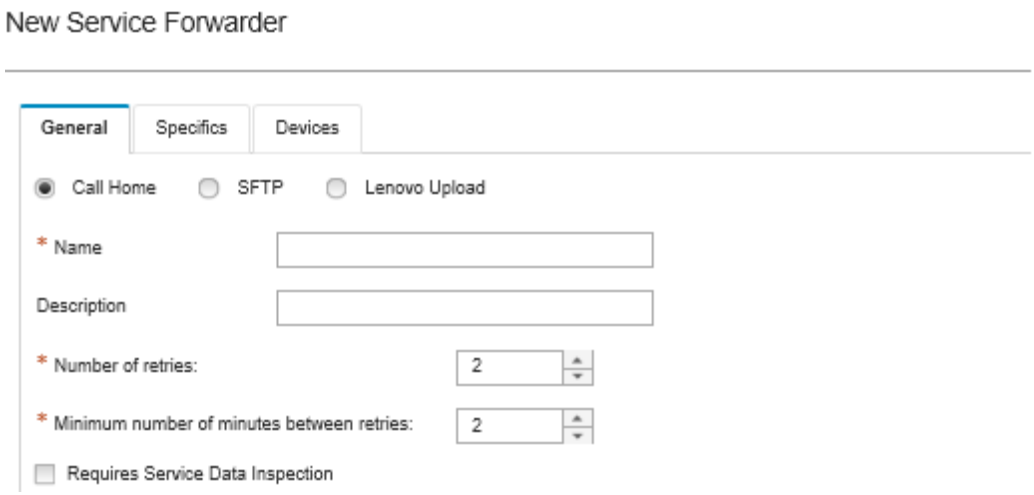
   Nota: Questa opzione non impedisce l'apertura manuale dei ticket di assistenza per i dispositivi con garanzie scadute
5. Compilare le informazioni di contatto e posizione.
6. Selezionare il metodo preferito per essere contattati dal supporto Lenovo.
7. (Facoltativo) compilare le informazioni di sistema.
8. Fare clic su **Applica**.

   Verrà creato un Call Home server d'inoltro di servizio denominato "Call Home predefinito" per tutti i dispositivi gestiti utilizzando le informazioni di contatto specificate.
9. Abilitare e testare il server d'inoltro di servizio "Call Home predefinito".
   a. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.
   b. Selezionare **Abilita** nella colonna **Stato** per il server d'inoltro di servizio "Call Home predefinito".
   c. Selezionare il server d'inoltro di servizio "Call Home predefinito" e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con il centro di assistenza Lenovo.

      Per monitorare l'avanzamento del test, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

      Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato

- Configurare Call Home per i dispositivi gestiti specifici:
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.
  2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.
  3. Fare clic sull'icona **Crea server d'inoltro di servizio** ( ) per visualizzare la finestra di dialogo "Nuovo server d'inoltro di servizio".
  4. Fare clic sulla scheda **Generale**.

     a. Selezionare **Call Home** come server d'inoltro di servizio:
     b. Immettere il nome del server d'inoltro di servizio e una descrizione.

c. Specificare il numero di tentativi di notifica automatici. Il valore predefinito è 2.

d. Specificare il numero minimo di minuti tra i tentativi. Il valore predefinito è 2.

e. (Facoltativo) Fare clic su **Ispezione dati di servizio necessaria** se si desidera controllare i file dei dati di servizio prima che vengano trasferiti e, facoltativamente, specificare l'indirizzo e-mail del contatto a cui inviare una notifica quando sarà necessario controllare i file di servizio.

5. Fare clic sulla scheda **Specifico** e compilare le informazioni di sistema e di contatto.

   Suggerimento: per utilizzare le stesse informazioni di contatto e posizione configurate nella pagina di configurazione di Call Home, selezionare **Configurazione generale** nel menu a discesa **Configurazione**.

6. Fare clic sulla scheda **Dispositivi** e selezionare i dispositivi gestiti e i gruppi di risorse per i quali si desidera che il server d'inoltro di servizio inoltri i file di servizio.

   Suggerimento: per inoltrare i file di servizio per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i dispositivi**.

7. Fare clic su **Crea**. Il server d'inoltro di servizio viene aggiunto alla pagina Assistenza e supporto.

8. Nella pagina Server d'inoltro di servizio, selezionare **Abilita** nella colonna **Stato** per abilitare il server d'inoltro di servizio.

9. Selezionare il server d'inoltro di servizio e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con il centro di assistenza Lenovo.

   Per monitorare l'avanzamento del test, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

   Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

Al termine

Dalla pagina Assistenza e supporto è inoltre possibile procedere come segue:

- Se l'opzione **Ispezione dati di servizio necessaria** è selezionata ed è stato ricevuto un evento che richiede assistenza da uno dei dispositivi gestiti associati al server d'inoltro di servizio, è necessario controllare i file di servizio prima che vengano inoltrati al fornitore di servizi. Per ulteriori informazioni, vedere .
- Determinare se Call Home è abilitato o disabilitato in un dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro e verificando lo stato nella colonna **Call Home Stato**.

  Suggerimento: se "Stato sconosciuto" viene visualizzato nella colonna **Call Home Stato**, aggiornare il browser Web per visualizzare lo stato corretto.
- Definire le informazioni di contatto e posizione di supporto per uno specifico dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Crea profilo di contatto** ( ) o sull'icona **Modifica profilo contatto** ( ). Le informazioni di contatto e posizione per il dispositivo gestito sono incluse nel ticket di assistenza che Call Home invia al Centro assistenza clienti Lenovo. Se vengono specificate informazioni di contatto e posizione univoche per un dispositivo gestito, verranno incluse nel ticket di assistenza. In caso contrario, verranno utilizzate informazioni generiche specificate per la configurazione XClarity Administrator Call Home (nella pagina **Call Home Configurazione** o **Server d'inoltro di servizio**). Per ulteriori informazioni, vedere Centro assistenza clienti Lenovo. Per ulteriori informazioni, vedere Definizione dei contatti di supporto per dispositivi specifici.
- Per visualizzare i ticket di assistenza inviati a Centro assistenza clienti Lenovo, fare clic su **Stato ticket di assistenza** nel riquadro di navigazione sinistro. In questa pagina sono elencati i ticket di assistenza aperti

automaticamente o manualmente da un server d'inoltro di servizio Call Home, lo stato e i file di servizio trasmessi al Centro assistenza clienti Lenovo. Per ulteriori informazioni, vedere Visualizzazione di ticket di assistenza e stato.

- Raccogliere i dati di servizio per uno specifico dispositivo facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Raccogli dati di servizio** ( ). Per ulteriori informazioni, vedere Raccolta e download dei dati di servizio per un dispositivo.
- Aprire manualmente un ticket di assistenza nel Centro assistenza clienti Lenovo, raccogliere i dati di servizio per uno specifico dispositivo e inviarli al Centro assistenza clienti Lenovo facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic su **Tutte le azioni → Esegui manualmente Call Home**.Se Centro assistenza clienti Lenovo richiede dati aggiuntivi, Supporto Lenovo potrebbe richiedere di raccogliere nuovamente i dati di servizio per il dispositivo specifico o per un altro dispositivo.

  Per ulteriori informazioni, vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo.
- Riabilitare Call Home in tutti i dispositivi gestiti facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro e quindi su **Tutte le azioni → Abilita Call Home su tutti i dispositivi**.

  Quando si abilita un server d'inoltro di servizio Call Home in Lenovo XClarity Administrator, Call Home è disabilitata in ogni dispositivo gestito, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi o si intende disabilitare Call Home in XClarity Administrator, è possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento.

Configurazione dell'invio di notifiche automatiche dei problemi alla Funzione Caricamento Lenovo

È possibile creare un server d'inoltro di servizio in grado di inviare automaticamente dati di servizio relativi di un dispositivo gestito al tecnico dell'assistenza Lenovo mediante la funzione Caricamento Lenovo, quando determinati eventi che richiedono assistenza, come un errore di memoria irrecuperabile, vengono ricevuti da specifici dispositivi gestiti, affinché il problema possa essere risolto. Il server d'inoltro di servizio è denominato "Funzione Caricamento Lenovo predefinita."

Lenovo è impegnata nella sicurezza. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nella Funzione Caricamento Lenovo è limitato al personale di assistenza autorizzato.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Verificare che tutte le porte richieste da Lenovo XClarity Administrator siano disponibili prima di configurare un server d'inoltro di servizio. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti dalla Funzione Caricamento Lenovo. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Nota: Se per lo stesso dispositivo sono configurati più server d'inoltro di servizio, uno solo di essi trasferisce i dati di servizio. L'e-mail e l'URL caricato utilizzati variano a seconda del server d'inoltro di servizio attivato per primo.

Informazioni su questa attività

Un *server d'inoltro di servizio* definisce le informazioni sulla destinazione dell'invio dei file di dati di servizio quando si verifica un evento che richiede assistenza. È possibile definire fino a 50 server d'inoltro di servizio.

- **Se un server d'inoltro di servizio per la funzione Caricamento Lenovo è configurato ma non abilitato**, è possibile trasferire *manualmente* i file di servizio raccolti alla funzione Caricamento Lenovo in qualsiasi momento. Per ulteriori informazioni, vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo.
- **Se un server d'inoltro di servizio Funzione Caricamento Lenovo è configurato e abilitato**, XClarity Administrator raccoglie *automaticamente* i dati di servizio e trasferisce il file di servizio a Funzione Caricamento Lenovo quando si verifica un evento che richiede assistenza per la risoluzione del problema.

  Per i Server ThinkSystem V3 e V4 (con XCC2 o XCC3), XClarity Administrator salva i dati di servizio in due file nel repository.

  – **File di servizio**. (.zip) Questo file contiene informazioni su servizio e inventario in un formato facilmente leggibile. Questo file viene inviato automaticamente alla Funzione Caricamento Lenovo quando si verifica un evento di manutenzione.

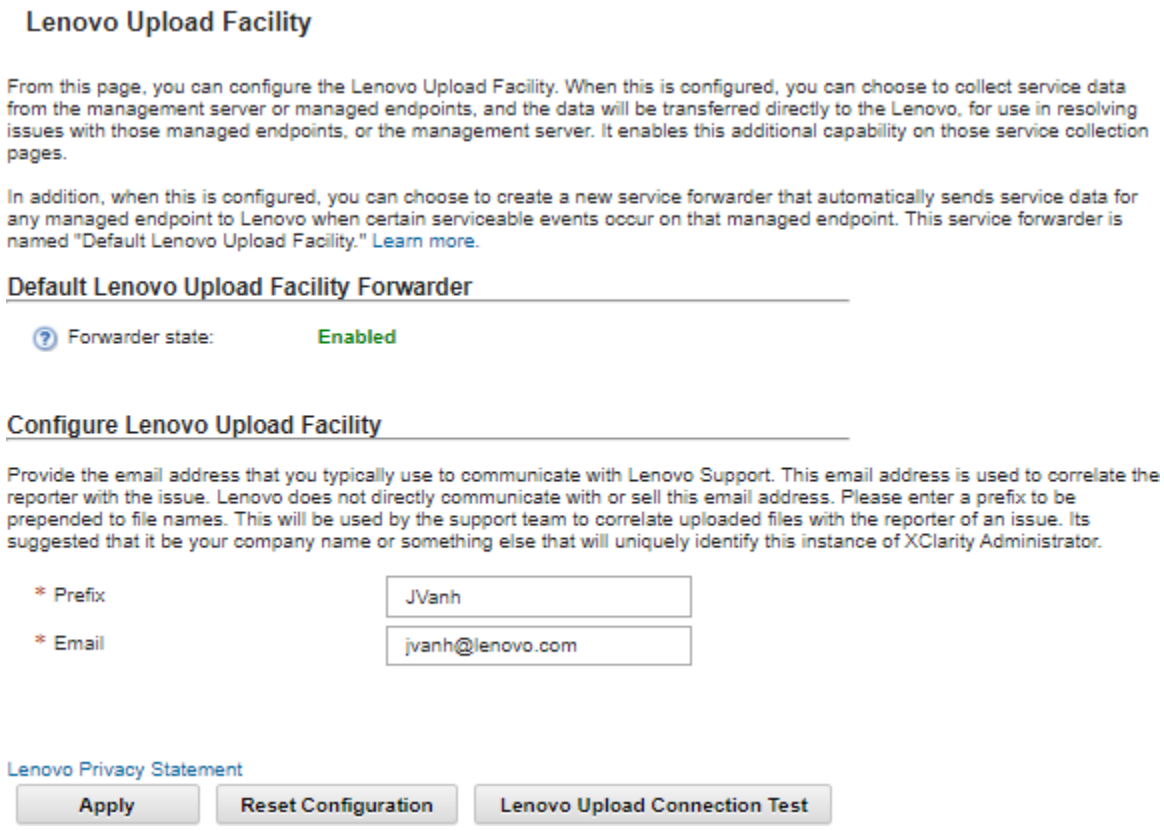
  – **File di debug**. (.tzz) Il file contiene tutte le informazioni sul servizio, l'inventario e i log di debug per l'utilizzo da parte del supporto Lenovo. È possibile inviare manualmente questo file al supporto Lenovo, se sono necessarie ulteriori informazioni per risolvere un problema.

  Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui informazioni su servizio, inventario e log di debug) in un singolo file di servizio nel repository. Questo file viene inviato alla Funzione Caricamento Lenovo quando si verifica un evento di manutenzione.

Procedura

Completare le seguenti operazioni per configurare un server d'inoltro di servizio per la funzione Caricamento Lenovo.

- Configurare un server d'inoltro di servizio per la funzione Caricamento Lenovo per tutti i dispositivi gestiti:
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.
  2. Fare clic su **Funzione Caricamento Lenovo** nel riquadro di navigazione sinistro per visualizzare la pagina Funzione Caricamento Lenovo.



3. Immettere l'indirizzo e-mail e l'URL forniti dal supporto Lenovo.
4. Fare clic su **Applica**.

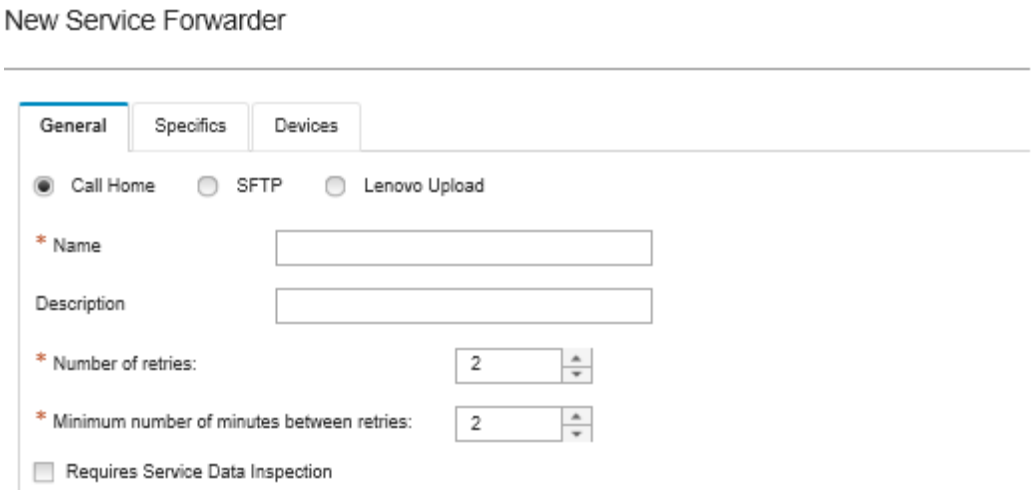
   Verrà creato un server d'inoltro di servizio denominato "Funzione Caricamento Lenovo predefinita" per tutti i dispositivi gestiti utilizzando le informazioni di contatto specificate.
5. Abilitare e testare il server d'inoltro di servizio per la "Funzione Caricamento Lenovo predefinita".
   a. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.
   b. Selezionare **Abilita** nella colonna **Stato** per il server d'inoltro di servizio "Funzione Caricamento Lenovo predefinita".
   c. Selezionare il server d'inoltro di servizio "Funzione Caricamento Lenovo predefinita" e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con la funzione Caricamento Lenovo.

      Per monitorare l'avanzamento del test, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

      Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

- Configurare un server d'inoltro di servizio per la funzione Caricamento Lenovo per specifici dispositivi gestiti:
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
  2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.

3. Fare clic sull'icona **Crea server d'inoltro di servizio** ( ) per visualizzare la finestra di dialogo Nuovo server d'inoltro di servizio.
4. Fare clic sulla scheda **Generale**.



   a. Selezionare **Caricamento Lenovo** per il server d'inoltro di servizio.
   b. Immettere il nome del server d'inoltro di servizio e una descrizione.
   c. Specificare il numero di tentativi di notifica automatici. Il valore predefinito è 2.
   d. Specificare il numero minimo di minuti tra i tentativi. Il valore predefinito è 2.
   e. (Facoltativo) Fare clic su **Ispezione dati di servizio necessaria** se si desidera controllare i file di servizio prima che vengano trasferiti e, facoltativamente, specificare l'indirizzo e-mail del contatto a cui inviare una notifica quando sarà necessario controllare i file di servizio.
5. Selezionare la scheda **Specifico** e compilare l'indirizzo e-mail e caricare l'URL fornito dal supporto Lenovo.
6. Fare clic sulla scheda **Dispositivi** e selezionare i dispositivi gestiti e i gruppi di risorse per i quali si desidera che il server d'inoltro di servizio inoltri i dati di servizio.

   Suggerimento: per inoltrare dati di servizio per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i dispositivi**.
7. Fare clic su **Crea**. Il server d'inoltro di servizio viene aggiunto alla pagina Assistenza e supporto.
8. Nella pagina Assistenza e supporto selezionare **Abilita** nella colonna **Stato** per abilitare il server d'inoltro di servizio.
9. Selezionare il server d'inoltro di servizio e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per ciascun server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di trasferire i dati alla funzione Caricamento Lenovo.

   Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

Al termine

Dalla pagina Assistenza e supporto è inoltre possibile procedere come segue:

- Se l'opzione **Ispezione dati di servizio necessaria** è selezionata ed è stato ricevuto un evento che richiede assistenza da uno dei dispositivi gestiti associati al server d'inoltro di servizio, è necessario controllare i file di servizio prima che vengano inoltrati al fornitore di servizi. Per ulteriori informazioni, vedere Ispezione dei file di servizio.

- Per modificare le informazioni d'inoltro di servizio, fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro e fare clic sull'icona **Modifica server d'inoltro di servizio** ( ).
- Per abilitare o disabilitare un fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare **Abilita** o **Disabilita** nella colonna **Stato**.
- Per eliminare il fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare l'icona **Elimina server d'inoltro di servizio** ( ).
- Raccogliere i dati di servizio per uno specifico dispositivo facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Raccogli dati di servizio** ( ). Per ulteriori informazioni, vedere Raccolta e download dei dati di servizio per un dispositivo.

Configurazione dell'invio di notifiche automatiche dei problemi al fornitore di servizi preferito

È possibile creare un server d'inoltro di servizio per inviare automaticamente i dati di servizio al fornitore di servizi preferito mediante SFTP, quando specifici dispositivi gestiti inviano determinati eventi che richiedono assistenza, come un errore di memoria irreversibile, al fine di risolvere il problema.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Accertarsi che tutte le porte richieste da XClarity Administrator (incluse le porte richieste per call home) siano disponibili prima di configurare un server d'inoltro di servizio. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti dal fornitore di servizi.

Se si sceglie di utilizzare Supporto Lenovo, accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Informazioni su questa attività

Un *server d'inoltro di servizio* definisce le informazioni sulla destinazione dell'invio dei file di dati di servizio quando si verifica un evento che richiede assistenza. È possibile definire fino a 50 server d'inoltro di servizio.

Per ogni server d'inoltro di servizio, è possibile scegliere di trasferire automaticamente i dati di servizio al supporto Lenovo (denominato *Call Home*), alla funzione Caricamento Lenovo oppure a un altro fornitore di servizi mediante SFTP. Per informazioni sulla configurazione di un server d'inoltro di servizio per Call Home, vedere Configurazione dell'invio di notifiche automatiche dei problemi. Per informazioni sulla configurazione di un server d'inoltro di servizio per la funzione Caricamento Lenovo, vedere Configurazione dell'invio di notifiche automatiche dei problemi alla Funzione Caricamento Lenovo.

Se un server d'inoltro di servizio è configurato e abilitato per SFTP, XClarity Administrator *trasferisce automaticamente* i dati di servizio raccolti e trasferisce i file di servizio al sito SFTP specificato per il fornitore di servizi preferito.

Per i Server ThinkSystem V3 e V4 (con XCC2 o XCC3), XClarity Administrator salva i dati di servizio in due file nel repository.

- **File di servizio**. (.zip) Questo file contiene informazioni su servizio e inventario in un formato facilmente leggibile. Questo file viene inviato automaticamente al fornitore di servizi preferito quando si verifica un evento di manutenzione.
- **File di debug**. (.tzz) Il file contiene tutte le informazioni sul servizio, l'inventario e i log di debug per l'utilizzo da parte del supporto Lenovo. È possibile inviare manualmente questo file al supporto Lenovo, se sono necessarie ulteriori informazioni per risolvere un problema.

Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui informazioni su servizio, inventario e log di debug) in un singolo file di servizio nel repository. Questo file viene inviato al fornitore di servizi preferito quando si verifica un evento di manutenzione.

Nota: Se per lo stesso dispositivo sono configurati più server d'inoltro di servizio SFTP, uno solo di essi trasferisce i dati di servizio. L'indirizzo e la porta utilizzati variano a seconda del server d'inoltro di servizio attivato per primo.

Procedura

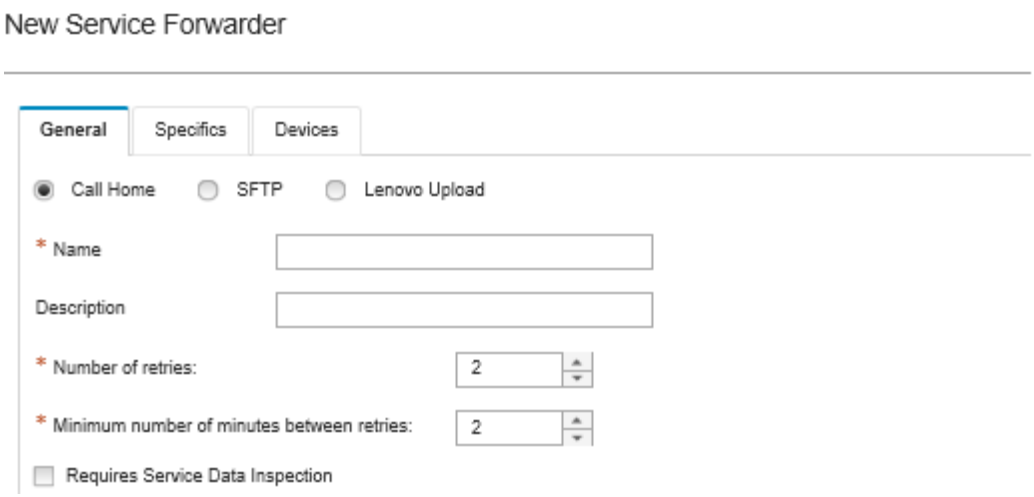
Per definire e abilitare un server d'inoltro di servizio, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.

Passo 3. Fare clic sull'icona **Crea server d'inoltro di servizio** ( ) per visualizzare la finestra di dialogo Nuovo server d'inoltro di servizio.

Passo 4. Fare clic sulla scheda **Generale**.



1. Selezionare **SFTP** per il server d'inoltro di servizio:
2. Immettere il nome del server d'inoltro di servizio e una descrizione.
3. Specificare il numero di tentativi di notifica automatici. Il valore predefinito è 2.
4. Specificare il numero minimo di minuti tra i tentativi. Il valore predefinito è 2.
5. (Facoltativo) Fare clic su **Ispezione dati di servizio necessaria** se si desidera controllare i file di servizio prima che vengano trasferiti e, facoltativamente, specificare l'indirizzo e-mail del contatto a cui inviare una notifica quando sarà necessario controllare i file di servizio.

Passo 5. Fare clic sulla scheda **Specifico** e compilare le seguenti informazioni:
- Indirizzo IP e numero di porta del server SFTP
- ID utente e password per l'autenticazione al server SFTP

Passo 6. Fare clic sulla scheda **Dispositivo** e selezionare i dispositivi gestiti e i gruppi di risorse per i quali si desidera che il server d'inoltro di servizio inoltri i dati di servizio.

Suggerimento: per inoltrare dati di servizio per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i dispositivi**.

Passo 7. Fare clic su **Crea**. Il server d'inoltro di servizio viene aggiunto alla pagina Assistenza e supporto

Passo 8. Nella pagina Assistenza e supporto selezionare **Abilita** nella colonna **Stato** per abilitare il server d'inoltro di servizio.

Passo 9. Per evitare che gli eventi che richiedono assistenza nell'elenco degli eventi esclusi aprano automaticamente report dei problemi, selezionare **No** accanto alla domanda **Si desidera che gli eventi esclusi siano in grado di aprire i report dei problemi?**

Passo 10. Selezionare il server d'inoltro di servizio e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con ciascun fornitore.

Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

Al termine

Dalla pagina Assistenza e supporto è inoltre possibile procedere come segue:

- Se l'opzione **Ispezione dati di servizio necessaria** è selezionata ed è stato ricevuto un evento che richiede assistenza da uno dei dispositivi gestiti associati al server d'inoltro di servizio, è necessario controllare i file di servizio prima che vengano inoltrati al fornitore di servizi. Per ulteriori informazioni, vedere Ispezione dei file di servizio.
- Per modificare le informazioni d'inoltro di servizio, fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro e fare clic sull'icona **Modifica server d'inoltro di servizio** ( ).
- Per abilitare o disabilitare un fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare **Abilita** o **Disabilita** nella colonna **Stato**.
- Per eliminare il fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare l'icona **Elimina server d'inoltro di servizio** ( ).
- Definire le informazioni di contatto e posizione di supporto per uno specifico dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Crea profilo di contatto** ( ) o sull'icona **Modifica profilo contatto** ( ). Le informazioni di contatto e posizione per il dispositivo gestito sono incluse nel record del problema creato da call home in Centro assistenza clienti Lenovo. Se vengono specificate informazioni di contatto e posizione univoche per un dispositivo gestito, verranno incluse nel record del problema. In caso contrario, verranno utilizzate informazioni generiche specificate per la configurazione call home di XClarity Administrator (nella pagina **Configurazione Call Home** o **Server d'inoltro di servizio**). Per ulteriori informazioni, vedere Definizione dei contatti di supporto per dispositivi specifici.
- Raccogliere i dati di servizio per uno specifico dispositivo facendo clic su **Azioni endpoint**, selezionando il dispositivo e quindi facendo clic sull'icona **Raccogli dati di servizio** ( ). Per ulteriori informazioni, vedere Raccolta e download dei dati di servizio per un dispositivo.

Per ulteriori informazioni su queste attività di assistenza e supporto, vedere Utilizzo di assistenza e supporto.

Modifica della password di ripristino del servizio

Se Lenovo XClarity Administrator non risponde e non può essere ripristinato, è possibile raccogliere e scaricare i dati di servizio e i log per questa istanza di XClarity Administrator. La password di ripristino del servizio è necessaria per accedere al servizio di raccolta e download dei dati.

Prima di iniziare

Per modificare la password, è necessario disporre dell'autorità **lxc-service-admin** o **lxc-supervisor**.

Nota: Assicurarsi di registrare la password per gli usi successivi. Non è possibile ripristinare un hub di gestione che non risponde senza utilizzare questa password.

Per ulteriori informazioni sull'utilizzo della password di ripristino del servizio, vedere Raccolta e download dei file di servizio per un'istanza Lenovo XClarity Administrator che non risponde.

Procedura

Per modificare la password di ripristino del servizio, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Password di ripristino del servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Password di ripristino del servizio.

Passo 3. Immettere la nuova password

Le password devono contenere da **16** a **256** caratteri, di cui uno o più caratteri speciali, numeri e caratteri alfabetici maiuscoli e minuscoli.

Passo 4. Fare clic su **Applica**.

Ispezione dei file di servizio

È possibile configurare un server d'inoltro di servizio per fare in modo che i file di servizio vengano ispezionati e accettati prima dell'invio.

Informazioni su questa attività

La colonna **Richiede attenzione** nella tabella del server d'inoltro di servizio indica se sono disponibili file di servizio che richiedono l'ispezione prima dell'inoltro al fornitore di servizi. Se sono disponibili per l'ispezione uno o più file di servizio, nella colonna viene visualizzato **Sì**; in caso contrario, viene visualizzato **No**.

Procedura

Per inoltrare specifici file di servizio al fornitore di servizi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare una tabella dei server d'inoltro di servizio.

Passo 3. Fare clic sul collegamento **Sì** nella colonna **Richiede attenzione** per visualizzare la finestra di dialogo Richiesta attenzione con un elenco dei file di servizio da analizzare.

Passo 4. Selezionare uno o più file di servizio e fare clic su **Scarica** per scaricare e analizzare il file.

Passo 5. Selezionare nuovamente uno o più file di servizio e fare clic su "Accetta" per avviare il trasferimento del file al fornitore di servizi configurato.

Nota: Se si sceglie **Rifiuta**, i file di servizio verranno rimossi dalla finestra di dialogo Richiede attenzione , ma rimarranno nel repository fino all'eliminazione.

Definizione dei contatti di supporto per dispositivi specifici

Specificare informazioni di contatto del supporto univoche per uno o più dispositivi specifici può essere utile nei casi in cui i dispositivi siano gestiti da più utenti.

Informazioni su questa attività

Se per un dispositivo sono definite informazioni di contatto del supporto, le informazioni specifiche del dispositivo sono incluse nei record dei problemi aperti automaticamente da Call Home per tale dispositivo. Se non sono definite informazioni specifiche del dispositivo, saranno incluse le informazioni di contatto generiche per Lenovo XClarity Administrator definite nella pagina **Server d'inoltro di servizio** o **Configurazione Call Home**.

Procedura

Per definire le informazioni di posizione e contatto del supporto per uno specifico dispositivo, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.

Passo 3. Selezionare uno o più dispositivi e fare clic sull'icona **Crea profilo di contatto** ( ) per visualizzare la finestra di dialogo Crea profilo di contatto.

Passo 4. Compilare i campi obbligatori e fare clic su **Salva**.

Al termine

Una volta definite le informazioni di contatto per un dispositivo, sarà possibile modificarle o eliminarle selezionando il dispositivo e facendo clic sull'icona **Modifica profilo contatto** ( ) o sull'icona **Elimina profilo contatto** ( ).

Nota: Se non esiste un profilo di contatto per il dispositivo selezionato, quando si tenta di modificare il profilo, viene visualizzata la finestra di dialogo Crea profilo di contatto.

Raccolta e download dei dati di servizio per un dispositivo

In presenza di un problema di un dispositivo gestito che richiede l'assistenza di un fornitore di servizi, è possibile utilizzare l'interfaccia Web di Lenovo XClarity Administrator per raccogliere manualmente i dati di servizio (inclusi informazioni sull'assistenza, inventario e log di debug) per il dispositivo, al fine di identificare l'origine del problema. I dati di servizio vengono salvati come file di servizio in formato tar.gz. È possibile scaricare o inviare i file di servizio al fornitore di servizi preferito.

Informazioni su questa attività

È possibile eseguire massimo 20 processi di raccolta dei dati di servizio alla volta.

Per i Server ThinkSystem V3 e V4 (con XCC2 o XCC3), XClarity Administrator salva i dati di servizio in due file nel repository.

- **File di servizio**. (.zip) Questo file contiene informazioni su servizio e inventario in un formato facilmente leggibile.
- **File di debug**. (.tzz) Il file contiene tutte le informazioni sul servizio, l'inventario e i log di debug per l'utilizzo da parte del supporto Lenovo.

Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui informazioni su servizio, inventario e log di debug) in un singolo file di servizio nel repository.

Quando un dispositivo gestito genera un evento che richiede assistenza che attiva la funzione Call Home (vedere Eventi hardware che avvisano automaticamente il supporto nella documentazione online di XClarity Administrator), XClarity Administrator raccoglie automaticamente i dati di servizio per tale dispositivo. Se è configurato e attivato un server d'inoltro di servizio, XClarity Administrator invia inoltre il file di servizio al fornitore di servizi specificato (ad esempio, al Centro assistenza clienti Lenovo mediante la funzione Call Home o un sito SFTP). Se il fornitore di servizi richiede dati aggiuntivi, potrebbe essere richiesto di raccogliere nuovamente i dati di servizio per il dispositivo specifico o per un altro, attenendosi alla procedura descritta di seguito.

Quando il repository dei dati di servizio raggiunge la sua capacità massima, per liberare spazio per il nuovo file verrà eliminato il set di file più obsoleto.

Nota:

- Per gli switch impilati, è possibile raccogliere i dati di servizio dello *switch principale* e degli *switch in standby* con indirizzi IP accessibili da XClarity Administrator. Non è possibile raccogliere dati di servizio per *switch membro* o in modalità protetta.
- Non è possibile raccogliere dati di servizio per switch che supportano la modalità stack ma sono in modalità autonoma.

Per informazioni su come scaricare i dati di servizio per XClarity Administrator, vedere Raccolta e download dei file di servizio Lenovo XClarity Administrator.

Per informazioni su come inviare manualmente i dati di servizio al Centro assistenza clienti Lenovo, vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo.

Per informazioni sulla configurazione di un server d'inoltro di servizio automatico, vedere Configurazione dell'invio di notifiche automatiche dei problemi.

Procedura

Per raccogliere e scaricare dati di servizio per un dispositivo gestito specifico, attenersi alla procedura descritta di seguito.

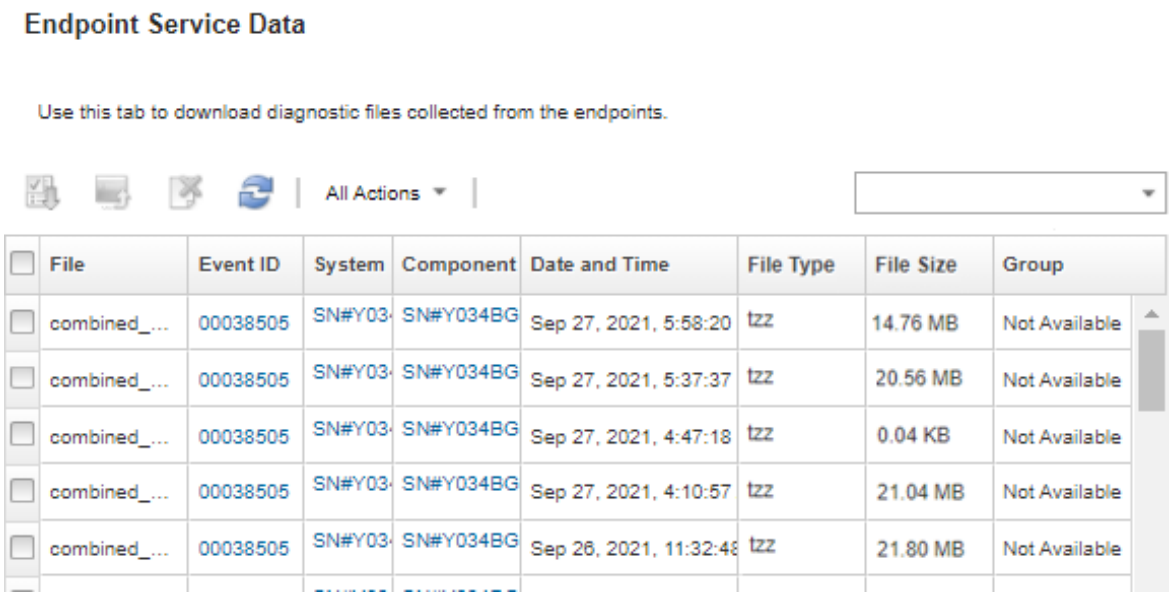
Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.

Passo 2. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.

Passo 3. Selezionare il dispositivo per cui si desidera raccogliere i dati di servizio e fare clic sull'icona **Raccogli dati di servizio** ( ).

Passo 4. Facoltativamente, salvare il file di servizio nel sistema locale.

Passo 5. Fare clic su **Dati di servizio dispositivo** nel riquadro di navigazione sinistro per visualizzare la pagina Dati di servizio dispositivo. L'archivio dei dati di servizio è elencato nella tabella.



Al termine

Dalla pagina Dati di servizio dispositivo è anche possibile eseguire queste attività.

- Inviare manualmente i file di servizio a un tecnico dell'assistenza Lenovo (vedere Trasferimento dei dati di servizio al supporto Lenovo).
- Inviare manualmente i file di servizio al centro di assistenza Lenovo e aprire un ticket di assistenza, vedere Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo.
- Allegare i file di servizio a un ticket di assistenza e inviarli al centro di assistenza Lenovo, selezionandoli e facendo clic su **Allega a ticket di assistenza**. Quindi selezionare il ticket di assistenza e fare clic su **Associa**.
- Scaricare i file di servizio selezionando uno o più file e facendo clic sull'icona **Scarica file di servizio selezionati** ( ). In caso di selezione multipla, i file vengono compressi in un unico file .tar.gz prima del download.
- Rimuovere i file di servizio non più necessari selezionando uno o più file e facendo clic sull'icona **Elimina file di servizio selezionati** ( ).

Raccolta e download dei file di servizio Lenovo XClarity Administrator

È possibile raccogliere manualmente i dati di servizio per Lenovo XClarity Administrator e i dispositivi gestiti specifici. Quindi, salvare le informazioni come file di servizio in formato tar.gz e scaricare o inviare i file di servizio al fornitore di servizi preferito per ottenere supporto per la risoluzione dei problemi in tempo reale.

Informazioni su questa attività

Nota: Accertarsi che *non* sia già in corso un processo di download di tutti i file di servizio (vedere Monitoraggio dei processi). Se un utente ha avviato un processo ancora in corso, dovrà attenderne il completamento prima di scaricare nuovamente tutti i file di servizio; in caso contrario, il secondo tentativo avrà esito negativo.

Contattare il Supporto Lenovo per stabilire se scaricare tutti o solo alcuni file di servizio oppure i log.

Nel repository vengono memorizzati fino a 100 file di servizio per XClarity Administrator.

Quando si scaricano i dati di servizio e i log di XClarity Administrator, è possibile includere i dati di servizio per dispositivi specifici nel file scaricato. È possibile scegliere di utilizzare i file di servizio esistenti o di raccogliere i dati di servizio correnti, nell'ambito del processo di download.

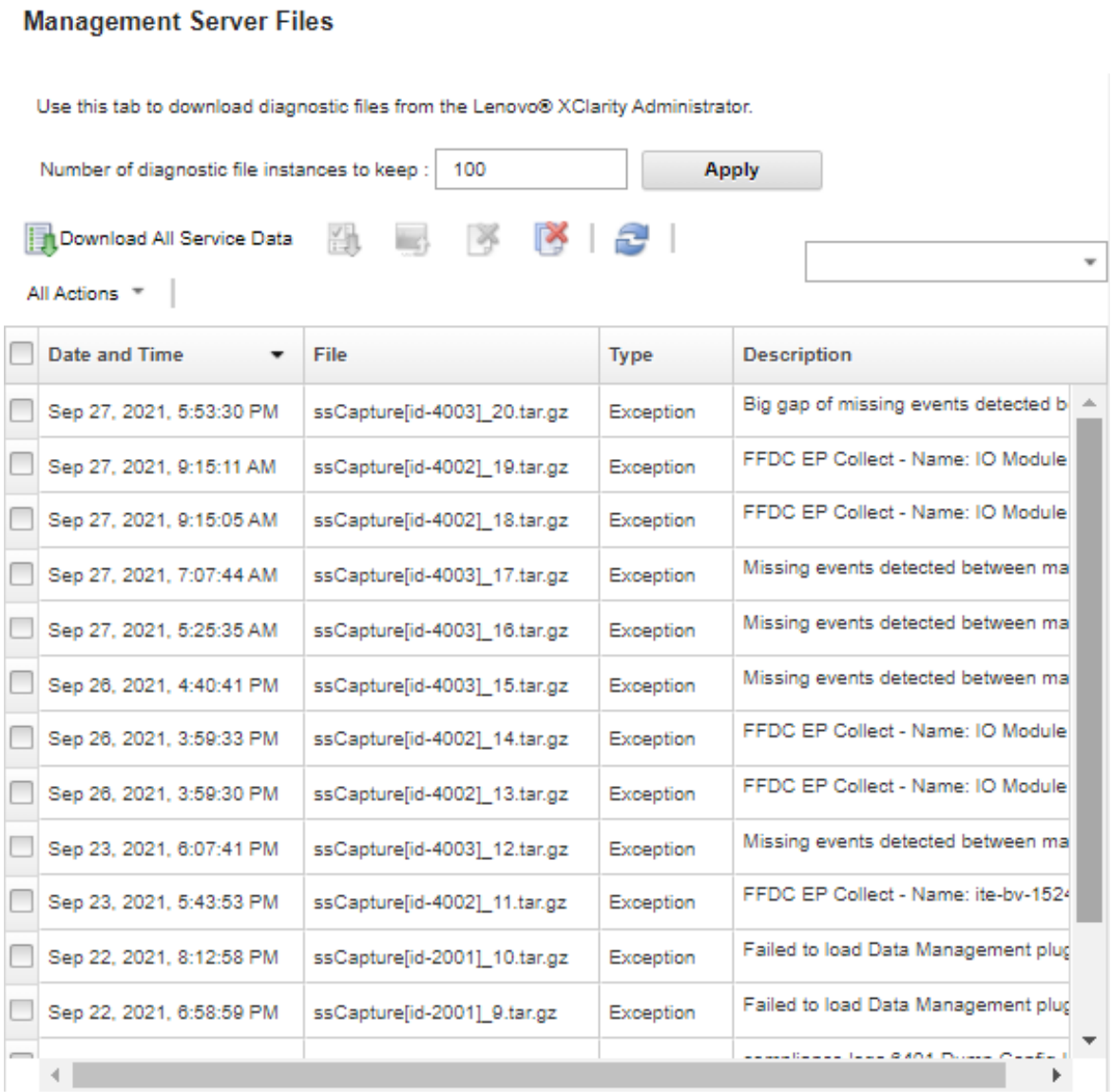
Attenzione: Non modificare il numero di file di servizio da mantenere, a meno che non si ricevano istruzioni specifiche dal fornitore di servizi.

Procedura

Per raccogliere e scaricare i log o i dati di servizio di XClarity Administrator, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.

Passo 2. Fare clic su **File server di gestione** nel riquadro di navigazione sinistro per visualizzare la pagina File server di gestione.



Passo 3. Scegliere di scaricare tutti i dati di servizio o tutti i log di servizio.

- Fare clic su **Scarica tutti i dati di servizio** per scaricare tutti i file di servizio, i log del server di gestione e i file di servizio di un dispositivo specifico.
- Fare clic su **Tutte le azioni → Scarica tutti i log di servizio** per scaricare tutti i log del server di gestione e i file di servizio di un dispositivo specifico.

Verrà visualizzato un messaggio che indica la quantità stimata di dati da scaricare. Il download dei file di servizio potrebbe richiedere molto tempo, in base al numero e alla dimensione dei file

Passo 4. Scegliere **Includi i dati di servizio già raccolti per i dispositivi gestiti**, selezionare i file di dati di servizio da includere e fare clic su **Applica**.

Passo 5. Scegliere **Selezionare i dispositivi gestiti per cui si desidera raccogliere nuovi dati di servizio**, selezionare i dispositivi di destinazione e quindi fare clic su **Applica**.

Passo 6. Decidere se inviare i file di servizio al supporto Lenovo oppure salvarli nel sistema locale o nello storage di rete. I dati di servizio o i file di log vengono compressi in un unico file .tar.gz prima di essere inviati.

- Se si fa clic su **Caricamento Lenovo**, facoltativamente è possibile immettere un numero di caso e quindi fare clic su **OK** per raccogliere e trasferire i file di servizio alla Funzione Caricamento Lenovo.

  Nota: Si consiglia di fornire il numero di caso per semplificare l'identificazione del file da parte del supporto Lenovo.
- Se si fa clic su **Salva in locale**, utilizzare le funzioni del browser Web per salvare il file nel sistema locale.
- Se si fa clic su **Salva in storage di rete**, specificare l'indirizzo IP, le credenziali, la directory e la porta e fare clic su Salva per trasferire i file di servizio al server remoto.

Al termine

Dalla pagina File server di gestione è inoltre possibile eseguire queste attività:

- Scaricare i file di servizio esistenti selezionando uno o più file e facendo clic su **Tutte le azioni → Scarica file di servizio selezionati**.

  È possibile scegliere di inviare i file di servizio al supporto Lenovo o di salvarli nel sistema locale o nello storage di rete. In caso di selezione multipla, i file vengono compressi in un unico file .tar.gz prima di essere inviati.
- Eliminare uno o più file di servizio selezionati, facendo clic sull'icona **Elimina file di servizio selezionati** ( ).
- Eliminare tutti i file di dati di servizio, facendo clic sull'icona **Cancella tutti i file di servizio** ( ).
- Eliminare tutti i log del server di gestione facendo clic su **Tutte le azioni → Cancella tutti i log di servizio**.

Raccolta e download dei file di servizio per un'istanza Lenovo XClarity Administrator che non risponde

Se Lenovo XClarity Administrator non risponde e non può essere ripristinato, è possibile raccogliere e scaricare i dati di servizio e i log per questa istanza di XClarity Administrator. I dati di servizio e i log vengano scaricati come un file di servizio in formato tar.gz nel sistema locale

Prima di iniziare

L'interfaccia Web XClarity Administrator è supportata dai browser Web che seguono.
- Chrome™ 48.0 o versioni successive (55.0 o versioni successive per la console remota)

- Firefox® ESR 38.6.0 o versioni successive
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o versioni successive (IOS7 o versioni successive e OS X)

Assicurarsi di eseguire il login all'interfaccia Web da un sistema con connettività di rete al sistema su cui è installato XClarity Administrator.

Procedura

Per raccogliere e scaricare i dati di servizio o i log per un'istanza XClarity Administrator che non risponde, completare le seguenti operazioni.

Passo 1. Puntare il browser all'indirizzo IP della macchina virtuale XClarity Administrator utilizzando il seguente URL.
`https://<IP_address>:58081`

Ad esempio:

`https://192.0.2.0:58081`

Passo 2. Specificare la password di ripristino del servizio nel campo **passKey**.

Questa è la password specificata durante la configurazione iniziale di XClarity Administrator o che è stata modificata nella scheda **Password di ripristino del servizio** nella pagina di assistenza e supporto (vedere "Modifica della password di ripristino del servizio " a pagina 72).

Passo 3. Selezionare i tipi di file che si desidera raccogliere.
- **Tutti i dati di servizio**. Consente di raccogliere tutti i file di servizio e i log del server di gestione.
- **Tutti i log di servizio**. Consente di raccogliere tutti i log del server di gestione.

Passo 4. Fare clic su **Raccogli** e utilizzare le funzioni del browser Web per salvare il file nel sistema locale. I dati di servizio o i file di log vengono compressi in un unico file .tar.gz prima di essere inviati.

Invio di una richiesta di servizio per problemi hardware al Centro assistenza clienti Lenovo

Se Call Home viene abilitato tramite un server d'inoltro e su un dispositivo gestito si verifica un evento che richiede assistenza, Lenovo XClarity Administrator apre automaticamente un ticket di assistenza, raccoglie i dati di servizio, li salva in un file di archivio e trasferisce il file di archivio del servizio a Funzione Caricamento Lenovo. Il file di archivio del servizio contiene i dati di servizio per il dispositivo e per XClarity Administrator. È inoltre possibile raccogliere e scaricare manualmente i file di servizio per un dispositivo gestito e inviarli al Centro assistenza clienti Lenovo in qualsiasi momento utilizzando XClarity Administrator. L'apertura di un ticket di assistenza avvia il processo atto a determinare una risoluzione dei problemi hardware rendendo le informazioni pertinenti disponibili per il Supporto Lenovo in modo rapido ed efficiente. I tecnici dell'assistenza Lenovo potranno iniziare a gestire la risoluzione in seguito al completamento e all'invio di un ticket di assistenza.

Lenovo è impegnata nella sicurezza. I dati di servizio che vengono in genere caricati manualmente sul supporto Lenovo vengono automaticamente inviati alla Funzione Caricamento Lenovo su HTTPS mediante TLS 1.2 o versione successiva. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nella Funzione Caricamento Lenovo è limitato al personale di assistenza autorizzato.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Accertarsi che le informazioni di contatto di call Home siano configurate.

1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
2. Fare clic su **Call Home Configurazione** nel riquadro di navigazione sinistro per visualizzare la pagina Configurazione Call Home.
3. Compilare le informazioni di contatto e posizione.
4. Facoltativo: compilare le informazioni di sistema.
5. Fare clic su **Applica**.

Accertarsi che tutte le porte richieste da XClarity Administrator (incluse le porte richieste per Call Home) siano disponibili prima di abilitare Call Home. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Informazioni su questa attività

Nella pagina Azioni endpoint, la colonna **Stato Call Home** indica se la funzione Call Home è abilitata nel controller di gestione della scheda di base. Un valore "Non applicabile" indica che Call Home non è supportato dal controller di gestione. XClarity Administrator è in grado di eseguire un'operazione Call Home per un dispositivo indipendentemente dal fatto che il controller di gestione supporti Call Home o meno. Per determinare se Call Home è supportato per uno specifico dispositivo, vedere la Supporto XClarity Administrator - Pagina Web sulla compatibilità.

Per ulteriori informazioni sulla configurazione e sull'abilitazione di Call Home per l'invio automatico di dati di servizio a Centro assistenza clienti Lenovo, vedere Configurazione dell'invio di notifiche automatiche dei problemi al supporto Lenovo (Call Home).

Per informazioni su come raccogliere e scaricare manualmente i dati di servizio, vedere Raccolta e download dei dati di servizio per un dispositivo e Raccolta e download dei file di servizio Lenovo XClarity Administrator.

Procedura

Per aprire manualmente un ticket di assistenza attenersi alla procedura descritta di seguito.

- Se la funzione Call Home è configurata ma non abilitata, eseguire i passaggi riportati di seguito per aprire un ticket di assistenza, raccogliere e scaricare i dati di servizio e inviare i file al Centro assistenza clienti Lenovo:
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
  2. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.
  3. Selezionare il dispositivo e fare clic su **Tutta l'azione → Esegui manualmente Call Home**.

Suggerimento: è possibile testare la comunicazione con il Centro assistenza clienti Lenovo per accertarsi che la funzione Call Home sia configurata correttamente senza inviare dati a Supporto Lenovo facendo clic su **Tutta l'azione → Esegui test Call Home**.

4. Fornire una descrizione del problema che si desidera segnalare, includendo gli ID degli eventi rilevanti.
5. Fare clic su **OK**.

- Se la funzione Call Home non è configurata o abilitata, è possibile inviare una richiesta di servizio contattando il supporto tecnico Lenovo. Per ulteriori informazioni, vedere Richiesta di supporto e assistenza tecnica .

Al termine

È possibile monitorare i ticket di assistenza dalla pagina **Stato ticket di assistenza** (vedere Visualizzazione di ticket di assistenza e stato).

Segnalazione dei problemi con XClarity Administrator

Quando si invia una richiesta di servizio per segnalare i problemi con il software (server di gestione), Lenovo XClarity Administrator apre un ticket di assistenza, raccoglie i dati di servizio dal server di gestione e invia i file al centro di assistenza Lenovo mediante la funzione Call Home. L'apertura di un ticket di assistenza avvia il processo di determinazione di una soluzione dei problemi software, mettendo a disposizione del supporto Lenovo le informazioni pertinenti in modo rapido ed efficiente. Una volta completato e aperto un ticket di assistenza, i tecnici dell'assistenza Lenovo potranno iniziare a lavorare alla risoluzione del problema.

Lenovo è impegnata nella sicurezza. I dati di servizio che vengono in genere caricati manualmente sul supporto Lenovo vengono automaticamente inviati al Centro assistenza clienti Lenovo su HTTPS mediante TLS 1.2 o versione successiva. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nel Centro assistenza clienti Lenovo è limitato al personale di assistenza autorizzato.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

- Prima di inviare una richiesta relativa a un problema per XClarity Administrator, considerare la possibilità di trovare una soluzione utilizzando le risorse seguenti:
  - Inviare idee e fornire feedback su XClarity Administrator facendo clic sul menu azioni utente ( ) sulla barra del titolo di XClarity Administrator, quindi su **Invia idee** o accedendo direttamente a Sito Web di Lenovo XClarity Ideation.
  - Porre domande e individuare le risposte facendo clic sul menu azioni utente ( ) sulla barra del titolo di XClarity Administrator, quindi su **Visita forum** o accedendo direttamente al Sito Web del forum della community dedicata a Lenovo XClarity.
  - Consultare Sito Web del supporto per i data center Lenovo per i più recenti suggerimenti e le tecniche da utilizzare per risolvere i problemi che si potrebbero riscontrare con XClarity Administrator. Questi *suggerimenti tecnici* descrivono le procedure per la risoluzione di problemi relativi all'utilizzo di XClarity Administrator.

    Per conoscere i suggerimenti tecnici disponibili per il server:

    1. Consultare Sito Web del supporto per i data center Lenovo.
    2. Immettere "XClarity Administrator" nel campo **Cerca**.
    3. Fare clic su **Visualizza tutto** nella sezione **Articoli principali** per visualizzare tutti i suggerimenti o immettere le parole chiave nel campo **Cerca** per trovare un suggerimento specifico.

Suggerimento: è possibile ordinare l'elenco di suggerimenti per **Pertinenza**, **Popolarità** o **Più recenti**.

- L'invio di una richiesta di servizio al supporto Lenovo per problemi correlati a XClarity Administrator richiede Lenovo XClarity Pro. Lenovo XClarity Pro dà diritto a usufruire del servizio di assistenza e supporto e a utilizzare la licenza di abilitazione di tutte le funzioni. Per ulteriori informazioni sull'acquisto di Lenovo XClarity Pro, contattare un rappresentante Lenovo o un business partner autorizzato.
- Accertarsi che il server d'inoltro **Call Home Lenovo predefinita** sia configurato e abilitato (vedere Configurazione dell'invio di notifiche automatiche dei problemi al supporto Lenovo (Call Home)).
- Accertarsi che tutte le porte richieste da XClarity Administrator (incluse le porte richieste per Call Home) siano disponibili prima di abilitare la funzione Call Home. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
- Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.
- Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Informazioni su questa attività

Se una richiesta Call Home è già in corso quando ne viene avviata una seconda, i dati vengono raccolti e inviati al supporto Lenovo per la prima richiesta Call Home, prima che i dati vengano raccolti e inviati per la seconda richiesta Call Home. Pertanto, potrebbe verificarsi un ritardo nell'invio dei dati per la seconda richiesta Call Home.

Procedura

Completare i seguenti passaggi per segnalare un problema con XClarity Administrator.

- Se la funzione Call Home è configurata, eseguire i passaggi riportati di seguito per aprire un ticket di assistenza, raccogliere e scaricare i dati di servizio per il server di gestione e inviare i file al centro di assistenza Lenovo:
  1. Dalla barra del titolo di XClarity Administrator, fare clic su **Segnala problema**. Il server di gestione esegue il test della connessione al supporto Lenovo.
  2. Fare clic su **Continua** per visualizzare la finestra di dialogo Informazioni sul problema software.
  3. Fornire il numero cliente Lenovo ricevuto al momento dell'acquisto di Lenovo XClarity Pro.
  4. Fornire le informazioni relative al problema, inclusi gli ID evento pertinenti e i dispositivi associati al problema.

     Nota:

     – I dati e i log di servizio per il server di gestione vengono raccolti e inviati automaticamente.
     – Se si selezionano i dispositivi associati al problema, vengono raccolti e inviati automaticamente anche i dati di servizio per i dispositivi.
     – È possibile allegare file aggiuntivi per semplificare la risoluzione dei problemi da parte del supporto Lenovo, come catture delle schermate e videoclip, facendo clic su **Carica file**.
  5. Fornire i passaggi per riprodurre il problema.
  6. Selezionare l'area funzionale in cui si è verificato il problema.
  7. Fare clic su **Avanti**.

8. Specificare le informazioni relative al contatto primario a cui rivolgersi per il problema. Per specificare i contatti aggiuntivi, fare clic su **Aggiungi un altro contatto**.
9. Fare clic su **Invia a Lenovo** per creare un ticket di assistenza con il supporto Lenovo.

- Se la funzione Call Home non è configurata o abilitata, è possibile inviare una richiesta di servizio contattando il supporto tecnico Lenovo. Per ulteriori informazioni, vedere Richiesta di supporto e assistenza tecnica .

Al termine

È possibile monitorare i ticket di assistenza dalla pagina **Stato ticket di assistenza** (vedere Visualizzazione di ticket di assistenza e stato).

È possibile allegare file aggiuntivi al ticket di assistenza aperto dopo l'invio del problema.

1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
2. Fare clic su **Stato ticket di assistenza** nel riquadro di navigazione sinistro per visualizzare la pagina Stato ticket di assistenza.
3. Selezionare il ticket di assistenza.
4. Fare clic su **Allega file di servizio** e selezionare l'archivio dei dati di servizio o un altro file che si desidera allegare al ticket di assistenza e inviarlo al supporto Lenovo.

Allegare un file di servizio a un ticket di assistenza aperto

È possibile allegare file di dati di servizio per un dispositivo specifico a un ticket di assistenza aperto nel Centro assistenza clienti Lenovo.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Informazioni su questa attività

È possibile allegare i file aggiuntivi per aprire un ticket di assistenza, come archivi dei dati di servizio correnti, catture delle schermate e videoclip.

Procedura

Per aggiungere un file di servizio a un ticket di assistenza aperto, attenersi alla procedura descritta di seguito.

- Dalla pagina **Dati di servizio dispositivo**:
  1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
  2. Fare clic su **Dati di servizio endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Dati di servizio endpoint.
  3. Selezionare il file di servizio che si desidera allegare a un ticket di assistenza.
  4. Fare clic su **Azioni → Allega a ticket di assistenza**, quindi selezionare il ticket di assistenza che si desidera allegare al file di servizio.
  5. Fare clic su **Associa** per allegare il file al ticket di assistenza e inviarlo al supporto Lenovo.
- Nella scheda **Stato ticket di assistenza**:

1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.
2. Fare clic su **Stato ticket di assistenza** nel riquadro di navigazione sinistro per visualizzare la pagina Stato ticket di assistenza.
3. Selezionare il ticket di assistenza.
4. Fare clic su **Allega file di servizio** e selezionare il file di servizio che si desidera allegare al ticket di assistenza e inviarlo al supporto Lenovo.

Visualizzazione di ticket di assistenza e stato

È possibile visualizzare le informazioni sulla creazione dei ticket di assistenza inviati manualmente e automaticamente al Centro assistenza clienti Lenovo mediante la funzione Call Home, come lo stato corrente e i file di servizio associati che sono stati trasferiti al Centro assistenza clienti Lenovo e i ticket di assistenza generati da servizi di supporto diversi da Call Home.

Procedura

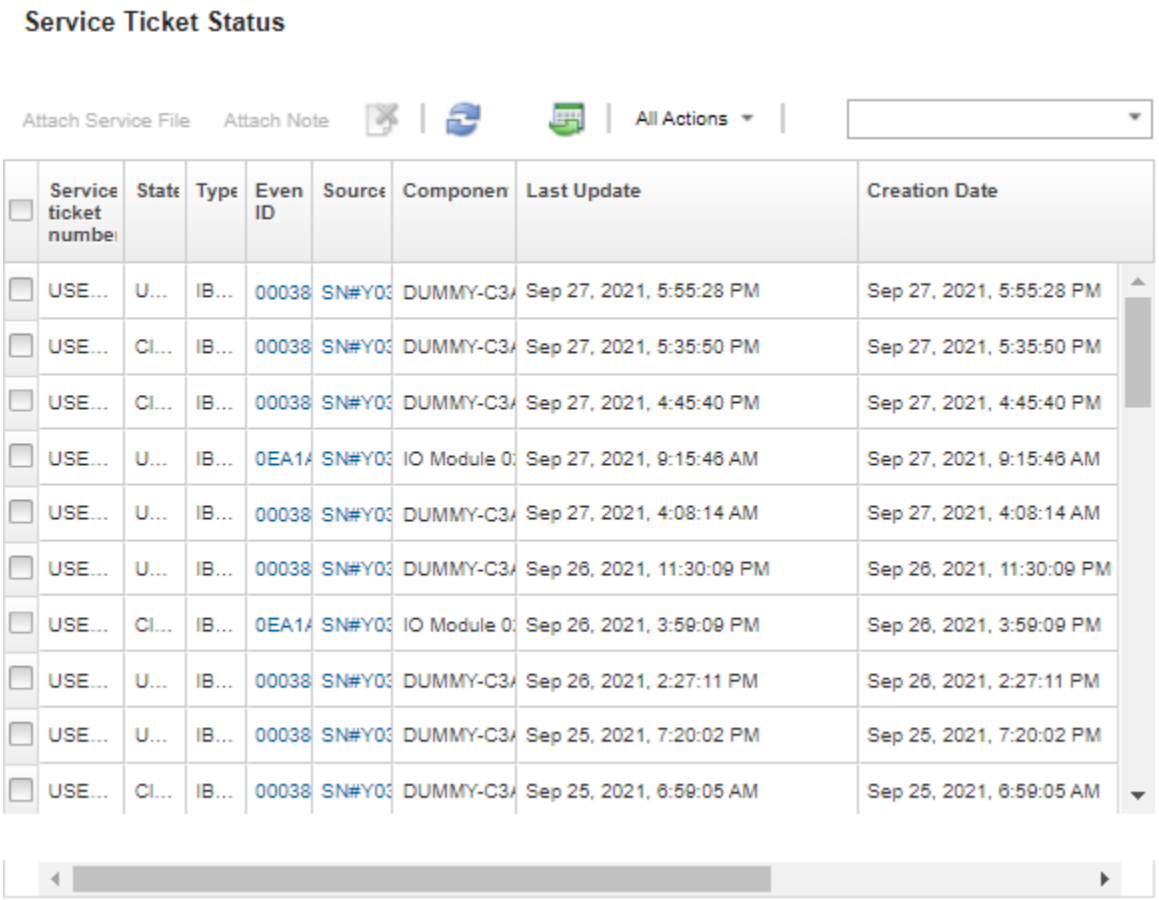
Per visualizzare i ticket di assistenza in XClarity Administrator, fare clic su **Amministrazione → Assistenza e supporto Stato ticket di assistenza** nel riquadro di navigazione sinistro per visualizzare la pagina Stato ticket di assistenza.

La colonna **Numero ticket di assistenza** mostra l'ID del ticket di assistenza aperto per un evento. Se sono stati aperti più ticket di assistenza per lo stesso evento (ad esempio, uno nel centro di supporto Lenovo e un altro in un ServiceNow Integrator), nella tabella sono presenti righe separate per ogni ticket di assistenza. È possibile trovare l'ID di un ticket di assistenza corrispondente nella colonna **ID di riferimento incrociato**. Ad esempio, se **Numero ticket di assistenza** mostra l'ID del ticket di assistenza del supporto Lenovo, l'**ID di riferimento incrociato** mostra l'ID del ticket di assistenza ServiceNow e viceversa.

La colonna **Tipo** identifica il tipo di ticket di assistenza elencato nella colonna **Numero ticket di assistenza**. Il tipo di ticket di assistenza può essere uno dei valori indicati di seguito.
- **Call Home IBM**
- **Test Call Home IBM**
- **Call Home Lenovo**
- **Test Call Home Lenovo**
- **Call Home software Lenovo**
- **Test Call Home software Lenovo**
- **Cherwill**
- **ServiceNow**

Un ticket di assistenza può trovarsi in uno dei seguenti stati:
- **Attivo**
- **Annullato**
- **Risolto**
- **Sconosciuto**

La colonna **ID di riferimento incrociato** contiene l'ID dei ticket di assistenza dei servizi di supporto esterni (come ServiceNow) correlati al ticket di assistenza Lenovo.



Al termine

Dalla pagina Stato ticket di assistenza è possibile completare le seguenti operazioni su un ticket di assistenza selezionato.

- Allegare un file di servizio per uno specifico dispositivo a un ticket di assistenza aperto al Centro assistenza clienti Lenovo facendo clic su **Allega file di servizio** (vedere Allegare un file di servizio a un ticket di assistenza aperto
- Allegare una nota per aprire un ticket di assistenza in Centro assistenza clienti Lenovo facendo clic su **Associa nota**.
- Per eliminare un ticket di assistenza fare clic sull'icona **Elimina ticket di assistenza** ( ). È possibile eliminare solo i ticket di assistenza il cui stato *non è* Attivo.
- Per recuperare le informazioni più recenti relative a tutti i ticket di assistenza dal Centro assistenza clienti Lenovo, fare clic sull'icona **Aggiorna stato ticket di assistenza** ( ).
- Esportare lo stato di tutti i ticket di assistenza in un file CSV facendo clic sull'icona **Esporta tutto come CSV** ( ).

Trasferimento dei dati di servizio al supporto Lenovo

Se si collabora con il supporto Lenovo per risolvere un problema, è possibile trasferire manualmente i file di servizio direttamente al rappresentante del supporto Lenovo mediante la funzione Caricamento Lenovo.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Procedura

Per trasferire i file di servizio direttamente al supporto Lenovo, attenersi alla procedura descritta di seguito.

Passo 1. Configurare la funzione Caricamento Lenovo.

a. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

b. Fare clic su **Funzione Caricamento Lenovo** nel riquadro di navigazione sinistro.

c. Immettere un indirizzo e-mail.

d. Fare clic su **Applica**.

Passo 2. Fare clic su **File server di gestione** o **Dati di servizio endpoint** nel riquadro di navigazione sinistro, a seconda dei log che è necessario inviare.

Passo 3. Selezionare uno o più file di servizio che si desidera inviare al supporto Lenovo e fare clic sull'icona **Caricamento Lenovo selezionato** ( ). Verrà visualizzata la finestra di dialogo Informazioni Caricamento Lenovo.

Passo 4. Facoltativamente, immettere un numero di caso.

Passo 5. Fare clic su **OK** per trasferire i file di servizio.

Configurazione delle impostazioni log del server di gestione

Le impostazioni log vengono utilizzate da Supporto Lenovo per regolare la granularità di registrazione solo se necessario.

Informazioni su questa attività

Attenzione: Non modificare le impostazioni in questa pagina, a meno che non si ricevano istruzioni dal Supporto Lenovo.

Procedura

Per configurare le impostazioni log, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Impostazioni di registrazione server** nel riquadro di navigazione sinistro per visualizzare la pagina Impostazioni di registrazione server.

Passo 3. Regolare ciascuna impostazione in base alle indicazioni del Supporto Lenovo e fare clic su **Applica**.

Al termine

Dalla pagina Impostazioni di registrazione server è anche possibile eseguire le seguenti operazioni.

- Scaricare le impostazioni di configurazione del log del server di gestione nel sistema locale facendo clic su **Scarica LogBack**. Le impostazioni vengono scaricate nella directory di download predefinita come file denominato logback.xml.
- Ripristinare le impostazioni predefinite facendo clic su **Ripristina valori predefiniti**.
- Importare un file di configurazione facendo clic su **Carica file di configurazione** e selezionando il file che si desidera importare in XClarity Administrator. Il file deve essere denominato logback.xml.

Importante: È consigliabile importare solo i file di configurazione forniti dal tecnico dell'assistenza Lenovo e solo seguendo le sue indicazioni.

Riabilitazione di Call Home su tutti i dispositivi gestiti

Quando si abilita un server d'inoltro di servizio Call Home in Lenovo XClarity Administrator, Call Home è disabilitata in ogni dispositivo gestito, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi o si intende disabilitare Call Home in XClarity Administrator, è possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento.

Informazioni su questa attività

Attenzione: La riabilitazione di Call Home su tutti i dispositivi non determina necessariamente il funzionamento di Call Home su di essi. Potrebbe esserne richiesta la configurazione su ciascun dispositivo, se precedentemente non è stata effettuata questa operazione.

Sebbene XClarity Administrator supporti la funzionalità Call Home per i dispositivi ThinkAgile e ThinkSystem, il controller di gestione della scheda di base per alcuni dispositivi ThinkAgile e ThinkSystem non include il supporto Call Home. Pertanto, non è possibile abilitare o disabilitare Call Home su questi dispositivi. Call Home può essere abilitato solo per i dispositivi al livello di XClarity Administrator.

Procedura

Per riabilitare Call Home su tutti i dispositivi gestiti, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.

Passo 3. Modificare lo stato di tutti i server d'inoltro di servizio Call Home, incluso quello "Call Home predefinito," in **Disabilitato**.

Passo 4. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.

Passo 5. Fare clic su **Tutte le azioni → Abilita Call Home in tutti i dispositivi** per abilitare Call Home in ciascun dispositivo gestito.

Invio di dati periodici a Lenovo

Facoltativamente, è possibile consentire a XClarity Administrator di raccogliere informazioni sull'utilizzo del prodotto e sulle modifiche dell'ambiente e di inviarle a Lenovo su base periodica. Lenovo utilizza questi dati per migliorare l'esperienza dei clienti con i prodotti e con il supporto Lenovo.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Informazioni su questa attività

È possibile raccogliere e inviare i seguenti tipi di dati a Lenovo.

- **Dati di utilizzo**

Analizzando i dati di utilizzo di più utenti, Lenovo può ottenere maggiori informazioni sull'utilizzo di XClarity Administrator. Ciò consente a Lenovo di conoscere le funzioni più utilizzate e di identificare i problemi che si verificano sulle istanze XClarity Administrator. Questi dati possono essere utilizzati per decisioni future sugli investimenti per migliorare i prodotti in base alle richieste dei clienti, per risolvere i problemi nelle versioni future e per migliorare la qualità dei prodotti.

Quando si accetta di inviare i dati di utilizzo a Lenovo, i seguenti dati vengono raccolti e inviati settimanalmente. Questi dati *sono anonimi*. Nessun dato privato (inclusi numeri di serie, UUID, nomi host, indirizzi IP e nomi utente) viene raccolto o inviato a Lenovo.
  - Log delle azioni eseguite
  - Elenco di eventi generati con relativa data/ora
  - Elenco di eventi di controllo generati con relativa data/ora
  - Elenco dei processi eseguiti e informazioni sull'esito positivo o negativo per ogni processo
  - XClarity Administrator metriche, come utilizzo della memoria, utilizzo del processore e spazio su disco
  - Dati di inventario limitati di tutti i dispositivi gestiti

- **Dati hardware**

  Analizzando i dati hardware di più utenti, Lenovo può acquisire informazioni sulle modifiche hardware regolari. Questi dati possono quindi essere utilizzati per migliorare le analisi predittive e l'esperienza di assistenza e supporto, approvvigionando le parti di ricambio nelle aree geografiche appropriate.

  Quando si accetta di inviare i dati hardware a Lenovo, i seguenti dati vengono raccolti e inviati periodicamente. Questi dati *non sono anonimi*. I dati hardware includono attributi, come UUID e numeri di serie. Non includono indirizzi IP o nomi host.

  - **Dati hardware quotidiani**. Per ogni modifica dell'inventario vengono inclusi i seguenti dati.
    - Evento di modifica dell'inventario (FQXHMDM0001I)
    - Modifiche dei dati di inventario per il dispositivo associato a tale evento
  - **Dati hardware settimanali**. I dati di inventario inclusi per tutti i dispositivi gestiti.

Quando i dati vengono inviati a Lenovo vengono trasmessi dall'istanza XClarity Administrator alla funzione Caricamento Lenovo mediante HTTPS. Le API REST vengono richiamate su questa connessione HTTPS per inviare i dati. Per l'autenticazione viene utilizzato un certificato precaricato su XClarity Administrator. Se un'istanza XClarity Administrator non ha accesso diretto a Internet ed è presente un proxy configurato in XClarity Administrator, i dati vengono trasmessi tramite questo proxy.

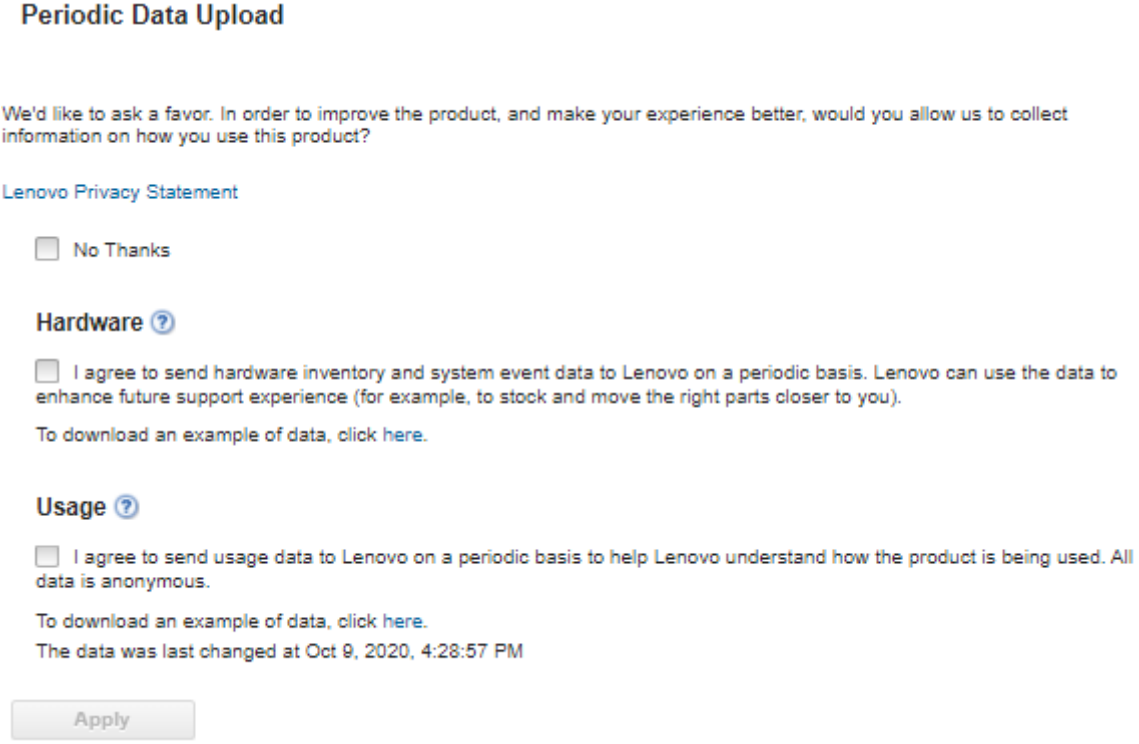
I dati vengono quindi spostati nel repository Lenovo Customer Care, dove vengono memorizzati per un massimo di 5 anni. Questo repository è una posizione sicura utilizzata anche quando i dati di debug vengono inviati a Lenovo per risolvere i problemi. Viene utilizzato dalla maggior parte dei prodotti server, storage e switch Lenovo.

Dal repository Lenovo Customer Care, le query vengono eseguite su tutti i dati relativi all'hardware e all'utilizzo e i grafici vengono resi disponibili per l'analisi da parte del team del prodotto Lenovo.

Procedura

Completare le seguenti operazioni per consentire a XClarity Administrator di raccogliere e inviare i dati dei clienti a Lenovo.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.



Passo 2. Fare clic su **Caricamento dati periodico** nel riquadro di navigazione sinistro per visualizzare la pagina Caricamento dati periodico.

Passo 3. Facoltativamente, accettare l'invio dei dati di utilizzo e hardware a Lenovo

Passo 4. Fare clic su **Applica**.

Al termine

Se si accetta di inviare i dati, da questa pagina è possibile eseguire le seguenti azioni.

- Determinare l'ultima volta che i dati sono stati inviati esaminando la data sotto la casella di controllo appropriata.
- Scaricare l'ultimo archivio dei dati inviato, facendo clic sul collegamento sotto la casella di controllo appropriata.

Dati di utilizzo di esempio

Gli esempi seguenti vengono raccolti e inviati periodicamente quando si accetta di inviare i dati di utilizzo a Lenovo.

Dati di metrica di XClarity Administrator

```
Timestamp   cpuLoad  usedSpace  usedRam  usedJavaCpu  usedJavaRam
1497861662  0.99     12.6225    13.3644  71.9         9.4
1497861668  1.23     12.6343    18.5676  0            14.4
1497861674  1.89     12.6371    19.6182  77.9         15.3
1497861679  1.98     12.6442    23.0782  37.9         18.6
1497861685  2.06     12.647     23.2412  77.9         18.6
1497861690  2.14     12.6654    25.3697  10           19
1497861696  2.37     7.75276    25.8952  2            19.4
1497861701  2.34     7.76077    26.0184  24           19.5
```

```
1497861056  2.55     7.77003    26.4222  85.9         19.7
1497861061  2.82     7.77877    26.5485  159.9        19.7
1497861067  3         7.7954     27.0066  131.9        20
```

Dati delle azioni

```
/updates/images/userdefined.png={"GET"\:1}
/config/profile={"GET"\:865}
/node/AD9547AB3C8011E79DCC000E1E7D4EE0={"GET"\:1}
/usage/data={"GET"\:12}
/compliancePolicies/persistedResult={"GET"\:3}
/jobs/88={"PUT"\:31}
/osdeployment/rest/internal/event/aicc={"POST"\:186}
/aicc={"GET"\:56}
/updates/images/powerStates.png={"GET"\:2}
/jobs/84={"PUT"\:3}
/updates/images/ActionSprite.png={"GET"\:1}
/nodes/AD9547AB3C8011E79DCC000E1E7D4EE0/lock={"GET"\:1,"PUT"\:2}
/updates/customUI/gridxExtensions/Mark.js={"GET"\:2}
/updates/images/ac22_deleteall_inactive_24.png={"GET"\:1}
/service/forwarders={"GET"\:12}
/nodes/7C64A0A8413811E7A6C6000E1EB35A90/lock={"GET"\:1,"PUT"\:2}
/config/deploy/status={"GET"\:865}
/node/235435543C7D11E7AA13000E1E7D54A0={"GET"\:1}
/updates/ApplyActivateUpdates.js={"GET"\:2}
/discovery={"GET"\:3}
/userAccountSettings={"GET"\:1}
/discoverRequest/jobs/610={"GET"\:9}
/compliancePolicies/events={"POST"\:25}
/events/audit={"GET"\:5}
/updates/images/st22_filterRunning_24.png={"GET"\:2}
/updates/images/st16_running_24.gif={"GET"\:1}
/updates/images/complianceStatus.png={"GET"\:2}
/usage={"GET"\:4}
/updates/json/firmwareRepository/exportPayloads.json={"GET"\:1}
/updates/images/ac22_collapseall_OneUI_24.png={"GET"\:3}
/chassis/0AC502DEFCD6419FB20FB5A9A49D0293={"GET"\:17}
/updates/images/ac22_copy_inactive_24.png={"GET"\:1}
/service/endPoint/collectedArchives={"GET"\:4}
/jobs/lock/88={"DELETE"\:1}
/updates/customUI/gridxModules/IndirectSelect.js={"GET"\:2}
/stgupdates/inventory/events={"POST"\:70}
/electronicDownload={"GET"\:1}
/updates/images/st16_firm_normal_24.png={"GET"\:3}
/updates/images/st16_Empty_24.png={"GET"\:1}
/updates/json/compliancePolicy/getCompByUxsp.json={"GET"\:1}
```

Dati di evento

```
{
   "action":100,
   "commonEventID":"FQXHMSE0203I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0203I",
   "flags":"",
   "mtm":"",
   "msgID":"",
   "service":100,
   "severity":200},
   "timeStamp":"2017-06-16T15:56:06Z"
}
```

Dati di controllo


```
{
   "action":100,
   "commonEventID":"FQXHMSE0200I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0200I",
   "flags":"",
   "msgID":"",
   "mtm":"",
   "service":100,
   "severity":200,
   "timeStamp":"2017-06-16T15:56:06Z"
}
```


Dati di inventario


```
-377665639={
   "firmwareList"\:[{
      "build"\:"2PET41C",
      "date"\:"2017-12-19T05\:00\:00Z",
      "name"\:"CMM firmware",
      "type"\:"CMM firmware",
      "version"\:""
   }],
   "mtm"\:"/",
   "productName"\:"",
   "stillManaged"\:"true",
   "uuid"\:"-377665639"
}
-177044123={
   "firmwareList"\:[{
      "build"\:"A3E117D",
      "date"\:"2018-01-26T00\:00\:00Z",
      "name"\:"UEFI Firmware/BIOS",
      "type"\:"UEFI",
      "version"\:"A3E117D-1.80"
   },{
      "build"\:"A3E113C",
      "date"\:"2016-12-16T00\:00\:00Z",
      "name"\:"UEFI Backup Firmware/BIOS",
      "type"\:"UEFI-Backup",
      "version"\:"A3E113C-1.60"
   },{
      "build"\:"DSALB1Q",
      "date"\:"2018-05-15T00\:00\:00Z",
      "name"\:"DSA Diagnostic Software",
      "type"\:"DSA",
      "version"\:"DSALB1Q-10.3"
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Firmware",
      "type"\:"IMM2",
      "version"\:"TCOO39A-4.70"
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Backup Firmware",
      "type"\:"IMM2-Backup",
      "version"\:"TCOO39A-4.70"
```

```
   }],
   "mtm"\:"7162/CC1",
   "productName"\:"Lenovo Flex System x240 Compute Node",
   "stillManaged"\:"true",
   "uuid"\:"-177044123"
}
-734000615={
   "firmwareList"\:[],
   "mtm"\:"8721/HC1",
   "productName"\:"IBM Flex System Enterprise Chassis Midplane Card"},
   "stillManaged"\:"true",
   "uuid"\:"-734000615"
1150304995={
   "firmwareList"\:[{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Boot ROM",
      "type"\:"Boot ROM",
      "version"\:"7.8.5.0"
   },{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Main Application 1",
      "type"\:"Main Application 1",
      "version"\:"7.8.5.0"
   },{
      "date"\:"03/29/2013",
      "build"\:"",
      "name"\:"Main Application 2",
      "type"\:"Main Application 2",
      "version"\:"7.5.3.0"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System Fabric EN4093 10Gb Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"1150304995"
}
-1050714125={
   "firmwareList"\:[{
      "date"\:"04/19/2016",
      "build"\:"",
      "name"\:"Main Application",
      "type"\:"Main Application",
      "version"\:"7.4.1c"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System FC5022 12-port 16Gb ESB SAN Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"-1050714125"
}
```


Dati hardware di esempio

L'esempio seguente viene raccolto e inviato periodicamente quando si accetta di inviare i dati hardware a Lenovo.

I dati vengono raccolti su base giornaliera e settimanale.

- "Dati hardware quotidiani" a pagina 92. Includono l'evento di modifica dell'inventario (FQXHMDM0001I) e le modifiche apportate all'inventario hardware per ogni modifica dell'inventario.
- "Dati hardware settimanali" a pagina 96. Includono l'inventario per tutti i dispositivi.

Dati hardware quotidiani


```
[{
    "2020-03-23T12:32:24.765": {
       "event": {
          "severity": 200,
          "timeStamp": "2020-03-23T16:32:21Z",
          "eventID": "FQXHMDM0001I",
          "eventClass": 800,
          "service": 100,
          "mtm": "",
          "flags": ["Hidden"],
          "action": 100,
          "msgID": "",
          "commonEventID": "FQXHMDM0001I",
          "cn": ""
       },
       "deviceInventoryChanges": [{
          "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36": [{
             "MODIFIED": [
                { "nodes": [] },
                { "accessState": "Pending" },
                { "powerSupplies": [{
                   "cmmDisplayName": "Power Supply 06",
                   "cmmHealthState": "Non-Critical",
                   "dataHandle": 0,
                   "description": "Power Supply",
                   "excludedHealthState": "Normal",
                   "firmware": [{
                      "build": "",
                      "classifications": [],
                      "date": "",
                      "name": "Power Supply Firmware",
                      "revision": "0",
                      "role": "",
                      "softwareID": "",
                      "status": "",
                      "type": "Power Supply Firmware",
                      "version": ""
                   }],
                   "FRU": "69Y5817",
                   "fruSerialNumber": "ZK125115V0VS",
                   "hardwareRevision": "5.0",
                   "healthState": "NA",
                   "inputVoltageMax": -1,
                   "inputVoltageIsAC": true,
                   "inputVoltageMin": -1,
                   "leds": [{
                      "color": "Green",
                      "location": "Planar",
                      "name": "OUT",
                      "state": "Off"
                   },
                   {
                      "color": "Amber",
                      "location": "Planar",
                      "name": "FAULT",
                      "state": "Off"
                   },
                   {
                      "color": "Green",
```

```
      "location": "Planar",
      "name": "IN",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2211",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Power Supply 06",
   "overallHealthState": "Normal",
   "parent": {
      "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
      "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
   },
   "partNumber": "69Y5801",
   "productName": "IBM 2500 W Power Supply",
   "posID": "60",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 343
   },
   "powerState": "Unknown",
   "productId": "303",
   "serialNumber": "",
   "slots": [6],
   "type": "PowerSupply",
   "userDescription": "",
   "uri": "powerSupply/04382F96885411E00095009500950095",
   "uuid": "04382F96885411E00095009500950095",
   "vpdID": "128"
},
{
   "cmmDisplayName": "Power Supply 04",
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "Power Supply",
   "excludedHealthState": "Normal",
   "firmware": [{
      "build": "",
      "classifications": [],
      "date": "",
      "name": "Power Supply Firmware",
      "revision": "5",
      "role": "",
      "softwareID": "",
      "status": "",
      "type": "Power Supply Firmware",
      "version": ""
   }],
   "FRU": "69Y5806",
   "fruSerialNumber": "ZK128116T03B",
   "hardwareRevision": "75.54",
   "healthState": "NA",
   "inputVoltageIsAC": true,
   "inputVoltageMax": 240,
   "inputVoltageMin": 220,
   "leds": [{
      "color": "Green",
      "location": "Planar",
      "name": "OUT",
```

```
            "state": "On"
         },
         {
            "color": "Amber",
            "location": "Planar",
            "name": "FAULT",
            "state": "Off"
         },
         {
            "color": "Green",
            "location": "Planar",
            "name": "IN",
            "state": "On"
         }],
         "machineType": "",
         "manufactureDate": "2511",
         "manufacturer": "IBM",
         "manufacturerId": "20301",
         "model": "",
         "name": "Power Supply 04",
         "overallHealthState": "Normal",
         "parent": {
            "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
            "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
         },
         "partNumber": "69Y5802",
         "productId": "304",
         "productName": "IBM 2500 W Power Supply",
         "powerAllocation": {
            "totalInputPower": 2505,
            "totalOutputPower": 343
         },
         "powerState": "Unknown",
         "posID": "61",
         "serialNumber": "",
         "slots": [4],
         "type": "PowerSupply",
         "userDescription": "",
         "uri": "powerSupply/FF2D840D7A644BCE91ADC16C78978A03",
         "uuid": "FF2D840D7A644BCE91ADC16C78978A03",
         "vpdID": "128"
      }]},
      { "fanMuxes": [{
         "cmmDisplayName": "Fan Logic 01",
         "cmmHealthState": "Non-Critical",
         "dataHandle": 0,
         "description": "Fan Logic Module",
         "excludedHealthState": "Normal",
         "FRU": "81Y2912",
         "fruSerialNumber": "Y031BG16D00S",
         "hardwareRevision": "4.0",
         "leds": [{
            "color": "Amber",
            "location": "FrontPanel",
            "name": "FAULT",
            "state": "On"
         }],
         "machineType": "",
         "manufacturer": "IBM",
         "manufactureDate": "2511",
         "manufacturerId": "20301",
```

```
                "model": "",
                "name": "Fan Logic 01",
                "overallHealthState": "Normal",
                "parent": {
                   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
                   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
                },
                "partNumber": "81Y2990",
                "productId": "338",
                "productName": "IBM Fan Pack Multiplexor Card",
                "status": "Non-Critical",
                "serialNumber": "",
                "slots": [1],
                "type": "FanMux",
                "uri": "fanMux/4247F859984711E08372E99E4175BAB0",
                "uuid": "4247F859984711E08372E99E4175BAB0"
             },
             {
                "cmmDisplayName": "Fan Logic 02",
                "cmmHealthState": "Non-Critical",
                "dataHandle": 0,
                "description": "Fan Logic Module",
                "excludedHealthState": "Normal",
                "FRU": "81Y2912",
                "fruSerialNumber": "Y031BG16D0CE",
                "hardwareRevision": "4.0",
                "leds": [{
                   "color": "Amber",
                   "location": "FrontPanel",
                   "name": "FAULT",
                   "state": "On"
                }],
                "machineType": "",
                "manufactureDate": "2511",
                "manufacturer": "IBM",
                "manufacturerId": "20301",
                "model": "",
                "name": "Fan Logic 02",
                "overallHealthState": "Normal",
                "parent": {
                   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
                   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
                },
                "productId": "338",
                "productName": "IBM Fan Pack Multiplexor Card",
                "partNumber": "81Y2990",
                "serialNumber": "",
                "slots": [2],
                "status": "Non-Critical",
                "type": "FanMux",
                "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
                "uuid": "71F72BE3985011E0B5A8E216694D6175"
             }]},
             { "switches": [] },
             { "excludedHealthState": "Normal" },
             { "overallHealthState": "Normal" },
             { "inventoryState": null }
          ]}
       ]
    }]
}
```

```
}]
```


Dati hardware settimanali


```
{
   "2020-03-23T12:41:28.045": {
      "cabinetList": [{
         "cabinetName": "STANDALONE_OBJECT_NAME",
         "chassisList": [{
            "itemName": "SN#Y010BG57Y01G",
            "itemUUID": "671D5D9EBB4440A49D9DAF08A9EDFB36",
            "itemParentUUID": "",
            "itemLocationRoom": "",
            "itemLocationRack": "",
            "itemLocation": "No Location ConfiguredL",
            "itemLowerUnit": 0,
            "itemType": "CHASSIS",
            "itemHeight": 10,
            "itemSubType": "unknown_type",
            "itemInventory": {
               "accessState": "Online",
               "activationKeys": [],
               "backedBy": "real",
               "bladeSlots": 14,
               "cmmDisplayName": "SN#Y010BG57Y01G",
               "cmmHealthState": "Non-Critical",
               "cmms": [{
                  "accessState": "Online",
                  "backedBy": "real",
                  "cmmDisplayName": "Standby CMM",
                  "dataHandle": 1584981183026,
                  "cmmHealthState": "Normal",
                  "description": "CMM",
                  "firmware": [{
                     "build": "1AON58O",
                     "classifications": [],
                     "date": "2020-03-20T04:00:00Z",
                     "name": "CMM firmware",
                     "revision": "58",
                     "role": "",
                     "status": "",
                     "type": "CMM firmware",
                     "version": "2.5.0"
                  }],
                  "FRU": "68Y7032",
                  "fruSerialNumber": "Y030BG168020",
                  "hostConfig": [],
                  "ipInterfaces": [{
                     "IPv4DHCPmode": "UNKNOWN",
                     "IPv4enabled": false,
                     "IPv6DHCPenabled": false,
                     "IPv6enabled": false,
                     "IPv6statelessEnabled": false,
                     "IPv6staticEnabled": false,
                     "label": "External",
                     "name": "eth0"
                  }],
                  "errorFields": [],
                  "excludedHealthState": "Normal",
                  "leds": [{
                     "color": "Amber",
```

```
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Standby CMM",
   "overallHealthState": "Normal",
   "partNumber": "68Y7054",
   "parent": {
      "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
      "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
   },
   "powerAllocation": {
      "maximumAllocatedPower": 20,
      "minimumAllocatedPower": 20
   },
   "productId": "65",
   "role": "backup",
   "serialNumber": "",
   "slots": [2],
   "type": "CMM",
   "uri": "cmm/F1F06BE6946511E089AEB9871E6892B2",
   "userDefinedName": "",
   "userDescription": "",
   "uuid": "F1F06BE6946511E089AEB9871E6892B2"
}],
"complex": [],
"contact": "No Contact Configured",
"dataHandle": 1584981227532,
"description": "Lenovo Flex System Chassis",
"displayName": "SN#Y010BG57Y01G",
"encapsulation": {
   "encapsulationMode": "normal"
},
"energyPolicies": {
   "acousticAttenuationMode": "Off",
   "hotAirRecirculation": {
      "chassisBay": [],
      "isEnabled": false,
      "maxVariation": 9.0
   },
   "powerCappingPolicy": {
      "cappingPolicy": "OFF",
      "currentPowerCap": 0,
      "maxPowerCap": 5010,
      "minPowerCap": 1504,
      "powerCappingAllocUnit": "watts"
   },
   "powerRedundancyMode": 4
},
"errorFields": [],
"excludedHealthState": "Warning",
"fanSlots": 10,
"fanMuxes": [{
   "cmmDisplayName": "Fan Logic 02",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 0,
   "description": "Fan Logic Module",
```

```
      "excludedHealthState": "Warning",
      "FRU": "81Y2912",
      "fruSerialNumber": "Y031BG16D0CE",
      "hardwareRevision": "4.0",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "On"
      }],
      "machineType": "",
      "manufactureDate": "2511",
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "model": "",
      "name": "Fan Logic 02",
      "overallHealthState": "Warning",
      "parent": {
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
      },
      "partNumber": "81Y2990",
      "productId": "338",
      "productName": "IBM Fan Pack Multiplexor Card",
      "serialNumber": "",
      "slots": [2],
      "status": "Non-Critical",
      "type": "FanMux",
      "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
      "uuid": "71F72BE3985011E0B5A8E216694D6175"
   }],
   "fanMuxSlots": 2,
   "fans": [{
      "cmmDisplayName": "Fan 06",
      "cmmHealthState": "Normal",
      "dataHandle": 0,
      "description": "IBM Fan Pack",
      "errorFields": [],
      "excludedHealthState": "Normal",
      "firmware": [{
         "build": "",
         "classifications": [],
         "date": "",
         "name": "Fan Controller",
         "revision": "226",
         "role": "",
         "status": "",
         "type": "Fan Controller",
         "version": "226"
      }],
      "FRU": "88Y6685",
      "fruSerialNumber": "YK10JPB69582",
      "hardwareRevision": "4.0",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "Off"
      }],
      "machineType": "",
      "manufactureDate": "2411",
```

```
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "model": "",
      "name": "Fan 06",
      "overallHealthState": "Normal",
      "parent": {
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
      },
      "partNumber": "88Y6691",
      "posID": "11",
      "powerAllocation": {
         "maximumAllocatedPower": 75,
         "minimumAllocatedPower": 75
      },
      "powerState": "Unknown",
      "productId": "342",
      "productName": "80mm Fan Pack for ITE Cooling",
      "serialNumber": "",
      "slots": [6],
      "type": "Fan",
      "userDescription": "",
      "uri": "fan/7293CA21938011E0BC13CB5D330B7C19",
      "uuid": "7293CA21938011E0BC13CB5D330B7C19",
      "vpdID": "373"
   }],
   "height": 10,
   "isConnectionTrusted": "true",
   "lastOfflineTimestamp": -1,
   "ledCardSlots": 1,
   "leds": [{
      "color": "Blue",
      "location": "FrontPanel",
      "name": "Location",
   "state": "Off"
   }],
   "location": {
      "location": "No Location ConfiguredL",
      "lowestRackUnit": 0,
      "rack": "",
      "room": ""
   },
   "machineType": "8721",
   "managerName": "UNKNOWN",
   "managerUuid": "UNKNOWN",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "mmSlots": 2,
   "model": "HC1",
   "name": "SN#Y010BG57Y01G",
   "nist": {
      "currentValue": "Compatibility",
      "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom","Compatibility"]
   },
   "nodes": [{
      "accessState": "Online",
      "activationKeys": [],
      "addinCards": [],
      "addinCardSlots": 0,
      "arch": "Unknown",
      "backedBy": "real",
```

```
"bladeState": 0,
"bladeState_health": "CRITICAL",
"bladeState_string": "Init failed",
"bootMode": {
   "currentValue": "",
   "possibleValues": []
},
"bootOrder": {
   "bootOrderList": [],
   "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)/bootOrder"
},
"cmmDisplayName": "Node 07",
"cmmHealthState": "Critical",
"complexID": -1,
"contact": "",
"dataHandle": 1584981175839,
"description": "",
"driveBays": 0,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
   "encapsulationMode": "notSupported"
},
"errorFields": [
   { "HostAndDomain": "NO_CONNECTOR" },
   { "PhysicalAndLocation": "NO_CONNECTOR" },
   { "Encapsulation": "NO_CONNECTOR" },
   { "Memory": "NO_CONNECTOR" },
   { "ServerFirmwareData": "NO_CONNECTOR" },
   { "RackCPU": "NO_CONNECTOR" },
   { "ServerOnboardPciDevices": "NO_CONNECTOR" },
   { "BootMode": "NO_CONNECTOR" },
   { "SecureBootMode": "NO_CONNECTOR" },
   { "BootOrder": "NO_CONNECTOR" },
   { "FlashDimm": "NO_CONNECTOR" },
   { "HostMacAddress": "NO_CONNECTOR" },
   { "VnicMode": "NO_CONNECTOR" },
   { "RemotePresenceEnabled": "NO_CONNECTOR" },
   { "ActivationKey": "NO_CONNECTOR" },
   { "LanOverUsbMode": "NO_CONNECTOR" },
   { "ServerStaticMetrics": "NO_CONNECTOR" },
   { "ScalableComplexPartitionUUIDData": "NO_CONNECTOR" },
   { "ActiveAlerts": "NO_CONNECTOR" },
   { "PFAConfiguration": "NO_CONNECTOR" },
   { "ServerIPaddresses": "NO_CONNECTOR"  },
   { "FaceplateInfo": "NO_CONNECTOR" },
   { "IOCompatibilityData": "NO_CONNECTOR" },
   { "LanOverUsbPortForwardingModes": "NO_CONNECTOR" },
   { "ServerConfigFiles": "NO_CONNECTOR" }
],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [],
"firmware": [],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "",
"hasOS": false,
```

```
"hostMacAddresses": "",
"ipInterfaces": [],
"isConnectionTrusted": "true",
"isITME": false
"isRemotePresenceEnabled": false,
"isScalable": false,
"lanOverUsb": "disabled",
"lanOverUsbPortForwardingModes": [],
"leds": [],
"location": {
   "location": "",
   "lowestRackUnit": 0,
   "rack": "",
   "room": ""
},
"logicalID": -1,
"m2Presence": false,
"machineType": "",
"manufacturer": "",
"manufacturerId": "",
"memoryModules": [],
"memorySlots": 0,
"mgmtProcType": "UNKNOWN",
"model": "",
"name": "Node 07",
"nist": {
   "currentValue": "Unknown",
   "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [],
"osInfo": {
   "description": "",
   "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partitionID": -1,
"partNumber": "",
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
   "maximumAllocatedPower": 0,
   "minimumAllocatedPower": 0
},
"powerStatus": 0,
"powerSupplies": [],
"primary": false,
"processors": [],
"processorSlots": 0,
"productId": "",
"productName": "",
"raidSettings": [],
"secureBootMode": {
   "currentValue": "",
   "possibleValues": []
},
```

```
    "securityDescriptor": {
       "managedAuthEnabled": false,
       "managedAuthSupported": true,
       "publicAccess": false,
       "roleGroups": ["lxc-supervisor"],
       "storedCredentials": {
          "description": "Credentials for null",
          "id": "1703",
          "userName": "USERID"
       },
       "uri": "nodes/dummy-671d5d9ebb4440a4-chassis(1)-blade(7)"
    },
    "serialNumber": "",
    "slots": [7],
    "status": {
       "message": "managed",
       "name": "MANAGED"
    },
    "subSlots": [],
    "subType": "",
    "tlsVersion": {
       "currentValue": "Unknown",
       "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
    },
    "type": "ITE",
    "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
    "userDefinedName": "",
    "userDescription": "",
    "uuid": "DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
    "vnicMode": "disabled",
    "vpdID": ""
}],
"overallHealthState": "Warning",
"parent": {
    "uri": "cabinet/",
    "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
    "allocatedOutputPower": 1504,
    "midPlaneCardMaximumAllocatedPower": 38,
    "midPlaneCardMinimumAllocatedPower": 38,
    "remainingOutputPower": 3506,
    "totalInputPower": 5445,
    "totalOutputPower": 5010
},
"powerSupplies": [{
    "dataHandle": 0,
    "cmmDisplayName": "Power Supply 06",
    "cmmHealthState": "Non-Critical",
    "description": "Power Supply",
    "excludedHealthState": "Warning",
    "firmware": [{
       "build": "",
       "classifications": [],
       "date": "",
       "name": "Power Supply Firmware",
       "revision": "0",
       "role": "",
```

```
      "softwareID": "",
      "status": "",
      "type": "Power Supply Firmware",
      "version": ""
   }                              ],
   "FRU": "69Y5817",
   "fruSerialNumber": "ZK125115V0VS",
   "hardwareRevision": "5.0",
   "healthState": "NA",
   "inputVoltageIsAC": true,
   "inputVoltageMax": -1,
   "inputVoltageMin": -1,
   "leds": [{
      "color": "Green",
      "location": "Planar",
      "name": "OUT",
      "state": "Off"
   }],
   "machineType": "",
   "manufactureDate": "2211",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Power Supply 06",
   "overallHealthState": "Warning",
   "parent": {
      "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
      "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
   },
   "partNumber": "69Y5801",
   "posID": "60",
   "powerAllocation": {
      "totalInputPower": 0,
      "totalOutputPower": 343
   },
   "powerState": "Unknown",
   "productId": "303",
   "productName": "IBM 2500 W Power Supply",
   "serialNumber": "",
   "slots": [6],
   "type": "PowerSupply",
   "uri": "powerSupply/04382F96885411E00095009500950095",
   "userDescription": "",
   "uuid": "04382F96885411E00095009500950095",
   "vpdID": "128"
}],
"powerSupplySlots": 6,
"productId": "336",
"productName": "IBM Chassis Midplane",
"securityDescriptor": {
   "managedAuthEnabled": false,
   "managedAuthSupported": true,
   "publicAccess": false,
   "roleGroups": ["lxc-supervisor"],
   "storedCredentials": {
      "description": "Credentials for null",
      "id": "1703",
      "userName": "USERID"
   },
   "uri": "chassis/671d5d9ebb4440a49d9daf08a9edfb36"
},
```

```
"SecurityPolicy": {
   "cmmPolicyState": "ACTIVE",
   "cmmPolicyLevel": "SECURE"
},
"serialNumber": "23DVG73",
"status": {
   "message": "MANAGED",
   "name": "MANAGED"
},
"switches": [{
   "accessState": "Online",
   "accessStateRecords": [{
      "health": "OFFLINE",
      "ipAddress": "10.241.53.20",
      "messageBundle": "com.lenovo.lxca.inventory.base.bundle.connections.messages",
      "messageDisplay": "Authentication failed occurred due to HTTP 401 - Unauthorized (OpenPegasus Error: \"U
      "messageID": "0510",
      "messageParameter": "HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
      "protocol": "CIM",
      "username": "USERID",
      "timestamp": 1584709239559,
      "trusted": true
   }],
   "attachedNodes": [],
   "backedBy": "real",
   "cmmDisplayName": "IO Module 04",
   "cmmHealthState": "Normal",
   "dataHandle": 1584981209777,
   "description": "FC5022 16Gb SAN Scalable Switch",
   "deviceName": "FC5022",
   "errorFields": [{
      "IOCompatibilityData": "FETCH_FAILED"
   }],
   "excludedHealthState": "Normal",
   "firmware": [{
      "classifications": [],
      "build": "",
      "date": "2016-04-19T04:00:00Z",
      "name": "Main Application",
      "status": "Active",
      "type": "Main Application",
      "version": "7.4.1c"
   }],
   "FRU": "00Y3329",
   "fruSerialNumber": "Y050UZ67D009",
   "ipInterfaces": [{
      "IPv4DHCPmode": "DHCP_THEN_STATIC",
      "IPv4enabled": true,
      "IPv6enabled": true,
      "IPv6DHCPenabled": true,
      "IPv6statelessEnabled": true,
      "IPv6staticEnabled": false,
      "label": "",
      "name": "ioe0"
   }],
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FRU Fault",
      "state": "Off"
   }],
```

```
            "machineType": "",
            "manufacturer": "LNV",
            "manufacturerId": "20301",
            "model": "",
            "name": "IO Module 04",
            "ntpPushEnabled": false,
            "ntpPushFrequency": 17,
            "overallHealthState": "Normal",
            "parent": {
               "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
               "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
            },
            "partNumber": "00MM452",
            "ports": [],
            "posID": "17",
            "powerAllocation": {
               "maximumAllocatedPower": -1,
               "minimumAllocatedPower": -1
            },
            "powerState": "On",
            "productId": "329",
            "productName": "Flex System FC5022 24-port 16Gb SAN Scalable Switch",
            "protectedMode": "Not supported",
            "securityDescriptor": {
               "managedAuthEnabled": false,
               "managedAuthSupported": true,
               "publicAccess": false,
               "roleGroups": [],
               "storedCredentials": {
                  "description": "Credentials for null",
                  "id": "1702",
                  "userName": "USERID"
               },
               "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6"
            },
            "serialNumber": "",
            "slots": [4],
            "stackMode": "N/A",
            "type": "Switch",
            "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6",
            "userDefinedName": "",
            "userDescription": "",
            "uuid": "AE986BEC1DD1B201684FC4F57C3B16B6",
            "vpdID": "309"
         }],
         "switchSlots": 4,
         "tlsVersion": {
            "currentValue": "TLS_12_Server",
            "possibleValues": ["TLS_12_Server","unsupported","TLS_12_Server_Client","SSL_30"]
         },
         "type": "Chassis",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
         "userDefinedName": "SN#Y010BG57Y01G",
         "userDescription": "",
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "vpdID": "336"
      }
   }],
   "complexList": [],
   "height": 52,
   "nodeList": [],
```

```
            "location": "",
            "placeholderList": [],
            "room": "",
            "storageList": [],
            "switchList": [],
            "UUID": "STANDALONE_OBJECT_UUID"
        }]
    }
}
```

Capitolo 4. Gestione dello spazio su disco

È possibile gestire la quantità di spazio su disco utilizzato da Lenovo XClarity Administrator, spostando i file di dati di grandi dimensioni non immediatamente necessari in una condivisione remota. In alternativa, è possibile eliminare le risorse non più necessarie.

Informazioni su questa attività

Per determinare lo spazio su disco attualmente utilizzato, fare clic su **Dashboard** dalla barra di menu di XClarity Administrator. L'utilizzo dello spazio sul disco del repository e delle condivisioni remote è riportato nella sezione Attività di XClarity Administrator.

Procedura

Completare una o più delle seguenti operazioni per liberare lo spazio su disco spostando i file su una condivisione remota ed eliminando le risorse non necessarie.

- **Eliminazione delle risorse non necessarie**

  È possibile eliminare rapidamente dal repository locale i file che non sono più necessari completando le seguenti operazioni.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Pulizia disco** per visualizzare la pagina Pulizia disco.
  2. Selezionare i file che si desidera eliminare. L'intestazione della sezione identifica la quantità di spazio che verrà liberata quando i file verranno eliminati.
     - **File correlati al sistema operativo**

       È possibile eliminare le immagini del sistema operativo, i file con opzioni di avvio e i file di software.
     - **Aggiornamenti firmware**

       È possibile eliminare i file di payload per tutti i driver di dispositivo del sistema operativo associati a UpdateXpress System Packs (UXSPs) e singoli driver di dispositivo con stato Scaricato.

       È possibile eliminare i file di payload per i singoli aggiornamenti firmware con stato Scaricato non utilizzati da un criterio di conformità del firmware.

       È possibile eliminare i file di payload del server di gestione con stato Scaricato.

       Nota: Quando il repository degli aggiornamenti firmware si trova in una condivisione remota, non è possibile utilizzare la funzione di pulizia del disco per eliminare i singoli aggiornamenti firmware e gli UXSP.
     - **File dei dati di servizio**

       Quando si verifica un evento di servizio su un dispositivo, i dati di servizio vengono raccolti automaticamente per tale dispositivo. I dati di servizio vengono automaticamente acquisiti per il server di gestione ogni volta che si verifica un'eccezione in XClarity Administrator. Si consiglia di eliminare periodicamente questi archivi se XClarity Administrator e i dispositivi gestiti sono in esecuzione senza problemi.

       Quando gli aggiornamenti del server di gestione vengono applicati correttamente, i file di aggiornamento vengono eliminati automaticamente dal repository.
  3. Fare clic su **Elimina elementi selezionati**.
  4. Esaminare l'elenco dei file selezionati e fare clic su **Elimina**.

© Copyright Lenovo 2015, 2025

- **La funzione di pulizia non ha utilizzato i pacchetti di aggiornamento firmware**

  È possibile eliminare tutti i pacchetti firmware inutilizzati nel repository degli aggiornamenti facendo clic su **Provisioning → Aggiornamenti firmware: Repository** nella barra dei menu di XClarity Administrator, quindi su **Tutte le azioni → Pulisci repository**.

  È possibile scegliere se conservare o rimuovere le versioni più recenti se non sono in uso.

  Viene creato un processo per espletare questa richiesta. Per monitorare l'avanzamento del processo, fare clic su **Monitoraggio → Processi** nella barra dei menu di XClarity Administrator.

- **Spostare i pacchetti di aggiornamento firmware in un repository remoto**

  Per impostazione predefinita, Lenovo XClarity Administrator utilizza un repository (interno) locale per gli aggiornamenti firmware disponibili. È possibile liberare lo spazio su disco disponibile nel repository locale XClarity Administrator utilizzando una condivisione remota montata su SSH File System (SSHTF) come repository remoto. È quindi possibile utilizzare i file di aggiornamento firmware direttamente dal repository remoto per mantenere la conformità del firmware sui dispositivi. Per ulteriori informazioni, vedere Utilizzo di un repository remoto per gli aggiornamenti firmware nella documentazione online di XClarity Administrator.

  Quando si modifica la posizione del repository degli aggiornamenti firmware, è possibile scegliere di copiare tutti gli aggiornamenti firmware dal repository originale al nuovo repository.

  I file di aggiornamento firmware nel repository originale *non vengono* puliti automaticamente dopo il cambio di posizione.

  Suggerimento: il repository degli aggiornamenti remoti può essere condiviso da più server di gestione XClarity Administrator.

  Per spostare gli aggiornamenti firmware in un repository degli aggiornamenti firmware remoto, completare le seguenti operazioni.

  1. Aggiungere una condivisione remota a XClarity Administrator (vedere Gestione delle condivisioni remote nella documentazione online di XClarity Administrator).
  2. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.
  3. Fare clic su **Tutte le azioni → Posizione repository switch** per visualizzare la finestra di dialogo Posizione repository switch.
  4. Selezionare la condivisione remota appena creata dall'elenco a discesa **Posizione repository**.
  5. Selezionare **Copia pacchetti di aggiornamento dal repository corrente nel nuovo repository** per copiare i file di aggiornamento firmware nella nuova posizione del repository prima di passare alla posizione del repository.
  6. Fare clic su **OK**.

     Viene creato un processo per copiare i pacchetti di aggiornamento firmware nel nuovo repository. Per monitorare l'avanzamento del processo, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.
  7. Pulire i file di aggiornamento firmware nel repository locale.
     a. Passare al repository locale facendo clic su **Tutte le azioni → Posizione repository switch**, selezionare **Repository locale** per la posizione del repository, quindi fare clic su **OK**.
     b. Fare clic sulla scheda **Aggiornamenti individuali**, selezionare la casella di controllo Seleziona tutto nella tabella per selezionare tutti gli aggiornamenti firmware, quindi fare clic sull'icona **Elimina pacchetti di aggiornamento completi** ( )

c. Fare clic sulla scheda **UpdateXpress System Pack (UXSP)**, selezionare la casella di controllo Seleziona tutto nella tabella per selezionare tutti gli UXSP, quindi fare clic sull'icona **Elimina UXSP e criterio associato** ( )

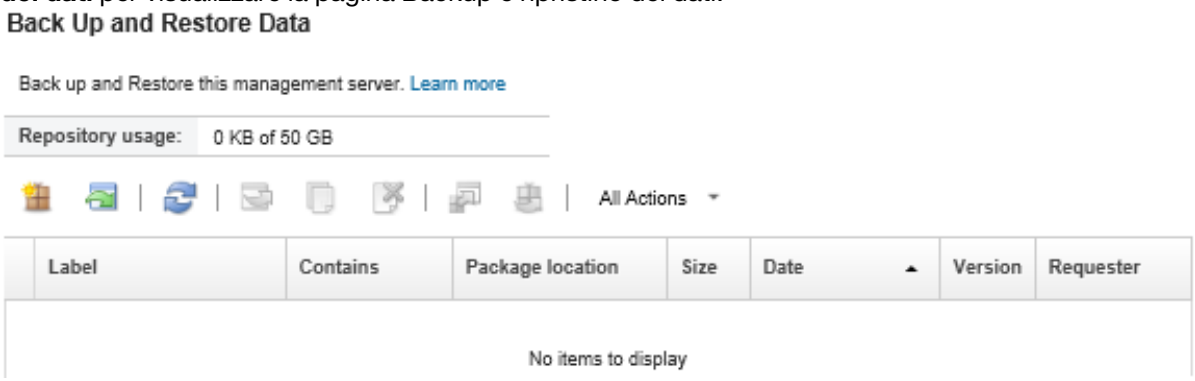
d. Tornare al repository remoto locale facendo clic su **Tutte le azioni → Posizione repository switch**, selezionare il nuovo repository remoto per la posizione del repository, quindi fare clic su **OK**.

- **Spostamento dei backup di XClarity Administrator in una condivisione remota**

  È possibile liberare spazio sul disco disponibile per il repository locale di XClarity Administrator spostando i backup di XClarity Administrator in una condivisione remota. Tuttavia, non è possibile utilizzare i file direttamente sulla condivisione remota. Per utilizzare i file, è necessario riportarli nel repository locale XClarity Administrator. Per ulteriori informazioni su condivisioni remote, vedere Gestione delle condivisioni remote nella documentazione online di XClarity Administrator.

  Importante: Si consiglia di scaricare i backup sul sistema locale o di copiare i backup in una condivisione remota prima di eliminare i backup in XClarity Administrator.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Backup e ripristino dei dati** per visualizzare la pagina Backup e ripristino dei dati.

     La colonna **Posizione pacchetto** indica se il backup è memorizzato in locale nel repository locale di XClarity Administrator o su una condivisione remota.

  2. Selezionare il backup e fare clic sull'icona **Copia backup** ( ) per visualizzare la finestra di dialogo Copia backup.
  3. Scegliere la condivisione remota per archiviare il backup.
  4. Fare clic su **Copia**.
  5. Monitorare l'avanzamento della copia nella pagina Processi. Una volta completata la copia, selezionare nuovamente il backup e fare clic sull'icona **Elimina backup** ( ) per visualizzare finestra di dialogo Elimina backup.
  6. Selezionare "Locale" per la posizione.
  7. Fare clic su **Elimina**.

Capitolo 5. Problemi di rilevamento e gestione

Utilizzare queste informazioni per risolvere i problemi di rilevamento e gestione dei dispositivi.

Impossibile rilevare un dispositivo

Utilizzare queste informazioni per risolvere i problemi durante il rilevamento di dispositivi gestibili.

1. Accertarsi che Lenovo XClarity Administrator supporti il dispositivo. Per un elenco di dispositivi supportati, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità, fare clic su sulla scheda **Compatibilità** e selezionare il collegamento per i tipi di dispositivo appropriati.
2. Accertarsi che il dispositivo sia raggiungibile in rete da XClarity Administrator e che XClarity Administrator sia raggiungibile in rete dal dispositivo.
3. Verificare che le porte corrette siano aperte nel firewall. Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
4. Accertarsi che nella rete siano abilitati i protocolli SLP unicast e multicast.
5. Per i server ThinkServer:
   a. Se si utilizza l'interfaccia Web di gestione per il server, verificare che il nome host del server sia configurato con un nome host o un indirizzo IP valido.
   b. Accertarsi che il protocollo SLP sia abilitato e che in ThinkServer System Manager (TSM) sia abilitato il nome host.
      - Per individuare i server ThinkServer con protocollo SLP abilitato, inviare una richiesta SLP di interrogazione del servizio WBEM utilizzando lo strumento SLP preferito.
        ```
        $ slptool findsrvs service:wbem
        service:wbem:http://<TSM_IP>:5988,65535
        service:wbem:https://<TSM_IP>:5989,65535
        ```
      - Per determinare se il protocollo SLP è abilitato in uno specifico server ThinkServer, inviare una richiesta SLP di interrogazione del servizio WBEM utilizzando lo strumento SLP preferito.
        ```
        $ slptool unicastfindattrs <TSM_IP> service:wbem
        (template-type=wbem),(template-version=2.0),(template-url-syntax=service:URL),
        (service-hi-name=qom),(service-hi-description=Quasi Object Manager 1.0.0),
        (CommunicationMechanism=cim-xml),(CommunicationMechanismsVersion=1.0),
        (MultipleOperationsSupported=false),(AuthenticationMechanismsSupported=Basic),
        (InteropSchemaNamespace=root/interop),(service-id=Lenovo G5 WBEM Service)
        ```
      - Se un dispositivo non risponde alla richiesta SLP, riavviare il firmware di TSM inviando un comando IPMI a TSM utilizzando i seguenti parametri. Il riavvio di TSM potrebbe richiedere alcuni minuti.
        ```
        NetFn = 0x06
        Command = 0x03
        Data = ()
        ```

        Nel seguente esempio, il protocollo SLP viene abilitato mediante lo strumento `ipmitool` open source.

        ```
        $ ipmitool -H <TSM_IP> -U <ipmi_user> -P <ipmipassword> raw 0x06 0x03
        ```
6. Per gli switch RackSwitch, accertarsi che il protocollo SLP sia abilitato e che il nome host sia impostato nella configurazione dello switch.
   - Impossibile trovare gli switch ThinkSystem serie DB. Per gestire questi switch, inserire manualmente l'indirizzo IP dello switch facendo clic su **Immissione manuale** nella pagina Rileva e gestisci nuovi dispositivi.

© Copyright Lenovo 2015, 2025

- Impossibile trovare gli switch NVIDIA Mellanox. Per gestire questi switch, inserire manualmente l'indirizzo IP dello switch facendo clic su **Immissione manuale** nella pagina Rileva e gestisci nuovi dispositivi.
- Per gli altri switch, accertarsi che il protocollo SLP sia abilitato e che il nome host sia impostato nella configurazione dello switch.
  - Per individuare gli switch con protocollo SLP abilitato, inviare la seguente richiesta SLP multicast utilizzando lo strumento SLP preferito.

    Nota: Questa richiesta individuerà solo gli switch che si trovano nella stessa sottorete in cui è in esecuzione lo strumento SLP.

    ```
    $ slptool findsrvs service:io-device.Lenovo:management-module
    service:io-device.Lenovo:management-module://<RackSwitch IP>,64225
    ```
  - Per determinare se il protocollo SLP è abilitato in uno specifico switch, inviare la seguente richiesta SLP unicast utilizzando lo strumento SLP preferito.
    ```
    $ slptool findattrs service:io-device.Lenovo:management-module://<RackSwitch IP>
    (level=1.0),(Type=switch),(data-protocols=ethernet),(serial-number=US7116000D),
    (sysoid=1.3.6.1.4.1.26543.1.7.6),(ipv4-enabled=TRUE),(ipv4-address=<RackSwitch IP>),
    (ipv6-enabled=FALSE),ipv6-addresses,(ipv4-mgmt-protocols=http:80:true,https:443:true,
    telnet:23:true,ssh:22:true,snmpv1v2v3:161:true,snmpv3only:161:false),
    (snmp-engineid=80:00:67:af:03:08:17:f4:33:d3),
    (ssh-fingerprint=8a:43:cb:be:47:d9:31:37:7a:3b:80:f6:dd:00:61:a6),
    (deviceName=<RackSwitch hostname>)
    ```

7. Per i dispositivi Lenovo Storage (diversi da ThinkSystem serie DE), verificare che il protocollo SLP sia abilitato e che la rete non blocchi la comunicazione SLP tra XClarity Administrator e il dispositivo di storage.
   - Per individuare i dispositivi di storage con protocollo SLP abilitato, inviare una richiesta SLP di interrogazione del servizio API utilizzando lo strumento SLP preferito.
     ```
     $ slptool findsrvs service:api
     service:api:https://<CONTROLLER_IP>:443/api,65535
     service:api:https://<CONTROLLER_IP>:443/api,65535
     ```
   - Per determinare se il protocollo SLP è abilitato in uno specifico dispositivo di storage, inviare una richiesta SLP di interrogazione del servizio API utilizzando lo strumento SLP preferito.
     ```
     $ slptool unicastfindattrs <CONTROLLER_IP> service:api
     (x-system-name=S3200_5.65),(x-system-location=rack\2Crack\2Crack),(x-system-contact=Support contact),
     (x-system-information=S3200_65),(x-vendor-name=Lenovo),(x-product-id=S3200),(x-product-brand=Storage),
     (x-midplane-serial-number=00C0FF2682A8),(x-platform-type=Gallium),(x-bundle-version=""),
     (x-build-date=""),(x-health=OK),(x-wwnn=208000c0ff2682a8),(x-mac-address=00:00:00:00:00:EB)
     ```

   Se un dispositivo di storage non risponde alla richiesta SLP:

   - Accertarsi che la rete consenta la comunicazione SLP tra i dispositivi.
   - Accertarsi che nei dispositivi di storage sia abilitata l'opzione **Storage Management Initiative Specification (SMI-S)** e riavviare il dispositivo di storage mediante l'interfaccia Web di gestione o la CLI.

Impossibile gestire un dispositivo

Utilizzare queste informazioni per risolvere i problemi durante la gestione dei dispositivi.

1. Accertarsi che il dispositivo sia supportato da Lenovo XClarity Administrator. Per informazioni sul supporto dei dispositivi, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità, fare clic su sulla scheda **Compatibilità** e selezionare il collegamento per i tipi di dispositivo appropriati.
2. Accertarsi che il dispositivo sia raggiungibile in rete da XClarity Administrator e che XClarity Administrator sia raggiungibile in rete dal dispositivo.

3. Verificare che tutte le porte idonee per la gestione siano aperte sulla rete e sui firewall. Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
4. Accertarsi che sia installato il firmware minimo richiesto in ciascun server che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.
5. Verificare che non vi siano problemi con il certificato del server XClarity Administrator.
   a. Verificare che il certificato del server XClarity Administrator non sia scaduto.
   b. Verificare che il certificato del server XClarity Administrator abbia un indirizzo IP valido in SubjectAltName (vedere Distribuzione dei certificati personalizzati dei server a XClarity Administrator nella documentazione online di XClarity Administrator).
6. Verificare che la data sul server non sia in conflitto con il certificato LDAP. Ad esempio, se il certificato LDAP è valido dal **3/8/2022** al **3/11/2024**, ma la data XCC è **15/04/2000**, il server non passerà il controllo TLS.
7. Accertarsi che nel dispositivo sia abilitato il protocollo CIM over HTTPS.
   a. Eseguire il login all'interfaccia Web di gestione per il server utilizzando l'account utente `RECOVERY_ID`.
   b. Fare clic su **Gestione IMM → Sicurezza**.
   c. Fare clic sulla scheda **CIM su HTTPS** e verificare che **Abilita CIM su HTTPS** sia selezionato.
8. Per i server ThinkSystem SR635 e SR655:
   - Verificare che sia installato un sistema operativo e che il server sia stato avviato sul sistema operativo, sul supporto avviabile montato oppure sulla shell EFI almeno una volta, in modo che XClarity Administrator possa raccogliere l'inventario per tali server.
   - Accertarsi che l'opzione IPMI su LAN sia abilitata. L'opzione IPMI su LAN è disabilitata per impostazione predefinita su questi server e deve essere abilitata manualmente prima di poter gestire i server. Per abilitare l'opzione IPMI su LAN mediante TSM, fare clic su **Impostazioni → Configurazione IPMI**. Per rendere effettiva la modifica potrebbe essere necessario riavviare il server.
9. Se il certificato del server del dispositivo è firmato da un'autorità di certificazione esterna, accertarsi che il certificato e gli eventuali certificati intermedi vengano importati nell'archivio attendibile di XClarity Administrator (vedere Distribuzione di certificati server personalizzati in dispositivi gestiti nella documentazione online di XClarity Administrator.
10. Verificare che le credenziali siano corrette per il dispositivo.

    Nota: Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.

    Se il dispositivo è gestito da XClarity Administrator, il controller di gestione viene inserito nella gestione centralizzata degli utenti. In altre parole, gli account utente definiti nel server di autenticazione interna o esterna di XClarity Administrator consentono inoltre di eseguire il login al controller di gestione. Verrà creato un nuovo account utente locale denominato RECOVERY_ID, mentre tutti gli altri account locali verranno disabilitati nel controller di gestione.

    Se il processo di gestione ha esito negativo durante la configurazione della gestione centralizzata degli utenti, gli account utente locali nel controller di gestione potrebbero essere disabilitati. Per ripristinare gli account utente locali, attenersi alla procedura descritta di seguito.

    - Server Converged, NeXtScale e System x
      a. Eseguire il login all'interfaccia Web di gestione per il server con l'account utente RECOVERY_ID.
      b. Fare clic su **Gestione IMM → Utente**.

c. Impostare il metodo di autenticazione utente nel controller di gestione su **Prima locale, quindi LDAP**.
   1) Fare clic su **Impostazioni di login globali**. Verrà visualizzata la finestra di dialogo Impostazioni di login globali.
   2) Fare clic sulla scheda **Generale**.
   3) Selezionare **Prima locale, quindi LDAP** per il metodo di autenticazione utente e fare clic su **OK**.

d. Eliminare e ricreare gli account utente locali (diversi dall'account utente RECOVERY_ID).

e. Tentare di gestire nuovamente lo chassis mediante l'opzione **Forza gestione** per rimuovere eventuali sottoscrizioni CIM rimanenti dal precedente tentativo di gestione.

- Chassis

a. Eseguire il login alla CLI di gestione per lo chassis da una sessione SSH con l'account utente RECOVERY_ID.

b. Eseguire il seguente comando per disabilitare la gestione centralizzata degli utenti e autenticare il controller di gestione e altri componenti dello chassis con gli account utente locali.

   Nota: Una volta eseguito questo comando, l'account utente RECOVERY_ID verrà rimosso dal Registro di sistema dell'utente e la sessione della CLI verrà terminata. È ora possibile eseguire l'autenticazione al controller di gestione e ad altri componenti dello chassis con gli account utente locali.

   ```
   fsmcm -off -T mm[p]
   ```

c. Tentare di gestire nuovamente lo chassis mediante l'opzione **Forza gestione** per rimuovere eventuali sottoscrizioni CIM rimanenti dal precedente tentativo di gestione.

11. Per gli switch RackSwitch
    - Accertarsi che nello switch sia abilitato il protocollo SSH
    - Se impostata, accertarsi che la password "enable" utilizzata per accedere alla modalità di esecuzione con privilegi nello switch sia corretta.
12. I server System x3950 X6 devono essere gestiti come due enclosure 4U, ciascuno con il proprio controller di gestione della scheda di base.
13. Se la scheda di sistema è stata sostituita nel dispositivo, con quest'ultimo è stato fornito un nuovo numero di serie e l'UUID. Se si desidera che XClarity Administrator riconosca il dispositivo come lo stesso prima della sostituzione, è necessario aggiornare il numero di serie e l'UUID in modo che corrispondano a quelli precedenti. Consultare la documentazione per le istruzioni sul dispositivo.
14. Se il dispositivo gestito da XClarity Administrator non è stato sottoposto ad annullamento della gestione, consultare le seguenti informazioni per i passaggi di ripristino:
    - Ripristino della gestione dello chassis con un modulo CMM dopo un errore del server di gestione nella documentazione online di XClarity Administrator
    - Ripristino della gestione del server dopo un errore del server di gestione nella documentazione online di XClarity Administrator
    - Ripristino di uno switch RackSwitch la cui gestione non è stata annullata correttamente nella documentazione online di XClarity Administrator
    - Ripristino della gestione con un dispositivo di storage Lenovo dopo un errore del server di gestione nella documentazione online di XClarity Administrator

Impossibile gestire un dispositivo di storage a causa di un certificato SSL TSL non valido

Utilizzare queste informazioni per risolvere i problemi durante la gestione degli array di storage.

Ogni dispositivo dispone di un certificato SSL autofirmato che utilizza Lenovo XClarity Administrator per comunicare con il dispositivo tramite HTTPS. Questo certificato presenta un nome comune (CN) che identifica il nome host (o l'indirizzo IP) associato al certificato. Il nome comune rappresenta il nome protetto dal certificato SSL e il certificato è valido solo se il nome host della richiesta corrisponde al nome comune del certificato. Pertanto, se l'indirizzo IP dell'array di storage viene modificato, il certificato esistente diviene non valido XClarity Administrator e non potrà gestirlo a causa di un certificato SSL/TSL non valido.

Per risolvere questo problema:

- Verificare che l'indirizzo IP nel valore CN del certificato inviato dal dispositivo di storage DE sia in formato IPv4.
- Verificare che il certificato SSL/TSL esistente sia valido.
  - Per gli array di storage Lenovo ThinkSystem DE, reimpostare il certificato di gestione sull'array di storage al certificato autofirmato predefinito. Per ulteriori informazioni, vedere Certificati di gestione delle reimpostazioni nella documentazione online di ThinkSystem Storage serie DE
  - Per gli array di storage Lenovo ThinkSystem DS, riavviare i controller di gestione nel dispositivo di storage mediante l'interfaccia Web di gestione o CLI per rigenerare il certificato con il CN corretto utilizzando il nuovo indirizzo IP o il nome host.

Impossibile gestire uno switch a causa di un certificato SSL TSL non valido

Utilizzare queste informazioni per risolvere i problemi relativi ai certificati, quando si gestiscono gli switch in esecuzione su CNOS.

Ogni dispositivo dispone di un certificato SSL autofirmato che utilizza Lenovo XClarity Administrator per comunicare con il dispositivo tramite HTTPS. Se si elimina o rigenera il certificato sullo switch, la comunicazione tra lo switch e XClarity Administrator non riuscirà e lo switch risulterà offline.

Per risolvere questo problema, dalla pagina "Tutti gli switch", selezionare lo switch e fare clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili**.

Impossibile ripristinare la connettività di uno chassis di Flex System gestito dopo la sostituzione della scheda LED posteriore o dell'assieme del midplane

Lenovo XClarity Administrator gestisce i dispositivi mediante il rispettivo UUID (Universally Unique Identifier) e il certificato attendibile basato su UUID. Per lo chassis di Flex System, l'UUID viene memorizzato come parte dei dati LED (Vital Product Data) sulla scheda LED posteriore che si trova sull'assieme del midplane. Quando si sostituisce la scheda LED posteriore o l'assieme del midplane, è necessario trasferire l'UUID delle schede LED posteriori sostituite alla nuova scheda LED posteriore.

1. Ottenere l'UUID dello chassis. Se lo chassis non funziona, è possibile ottenere l'UUID contattando il supporto e fornendo il tipo di macchina e il numero di serie, riportati su una delle etichette dello chassis.
2. Modificare l'UUID di uno chassis. Vedere Documentazione online di Lenovo Flex System per il dispositivo in uso per la sostituzione della scheda LED posteriore e le istruzioni per la modifica dell'UUID.
3. Risolvi certificati non attendibili per lo chassis.
   a. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Chassis**. Viene visualizzata la pagina Tutti gli chassis.
   b. Selezionare lo chassis con la parte sostituita.
   c. Fare clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili**.

d. Fare clic su **Installa certificato**.

XClarity Administrator recupera il certificato corrente dallo chassis di destinazione e lo salva nell'archivio attendibile di XClarity Administrator, sovrascrivendo il certificato precedente per lo chassis.

4. Aggiornare l'inventario per lo chassis, facendo clic su **Tutte le azioni → Inventario → Aggiorna inventario**.

Impossibile ripristinare la connettività di un server gestito dopo la sostituzione della scheda di sistema

Lenovo XClarity Administrator gestisce i dispositivi mediante il rispettivo UUID (Universally Unique Identifier) e il certificato attendibile basato su UUID. Per i server, l'UUID viene memorizzato come parte dei dati VPD (Vital Product Data) sulla scheda di sistema. Quando si sostituisce la scheda di sistema, è necessario trasferire l'UUID della scheda di sistema sostituita sulla nuova scheda di sistema.

Importante: Si consiglia di annullare la gestione del server prima di sostituire la scheda di sistema. Una volta sostituita la scheda di sistema è quindi possibile gestire nuovamente il server.

Completare le seguenti operazioni per trasferire l'UUID della scheda di sistema sostituita sulla nuova scheda di sistema.

1. Ottenere l'UUID del server. Se il server non funziona, è possibile ottenere l'UUID contattando il supporto e fornendo il tipo di macchina e il numero di serie, riportati su una delle etichette del server.
2. Modificare l'UUID di un server. Consultare il manuale hardware del dispositivo in uso per la sostituzione del componente e le istruzioni per la modifica dell'UUID.
3. Risolvi certificati non attendibili per il server.
   a. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Tutti gli chassis.
   b. Selezionare il server con la parte sostituita.
   c. Fare clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili**.
   d. Fare clic su **Installa certificato**.

   XClarity Administrator recupera il certificato corrente dal server di destinazione e lo salva nell'archivio attendibile di XClarity Administrator, sovrascrivendo il certificato precedente per il server.
4. Aggiornare l'inventario per il server, facendo clic su **Tutte le azioni → Inventario → Aggiorna inventario**.

Incapsulamento non disabilitato dopo l'annullamento della gestione di un server

Se è abilitato l'incapsulamento globale, la modalità di incapsulamento viene impostata sull'"incapsulamento lite" durante la gestione di un server. In genere, quando si annulla la gestione del server, viene ripristinata la modalità di incapsulamento "normale" (disabilitata).

Se la modalità di incapsulamento non passa a "normale", attenersi alla procedura descritta di seguito per disabilitare l'incapsulamento:

1. Riavviare il controller di gestione della scheda di base.
2. Connettersi al server di destinazione da un sistema configurato per l'utilizzo dell'indirizzo IP dell'appliance virtuale Lenovo XClarity Administrator con errori. Disabilitare quindi l'incapsulamento aprendo una sessione SSH nel dispositivo ed eseguendo il seguente comando:
   ```
   encaps lite off
   ```

Il nodo di elaborazione non viene visualizzato nell'interfaccia utente dopo la gestione

Se si sostituisce un server ThinkSystem SD530 in uno chassis senza prima annullare la gestione esistente, il nuovo server potrebbe non essere visualizzato nell'interfaccia utente.

Per risolvere questo problema, annullare la gestione dello chassis utilizzando l'opzione "Forza" e quindi gestire nuovamente il server ThinkSystem SD530 in uno chassis.

Lo stato di alimentazione del server non è corretto

Se è acceso un server senza sistema operativo, Lenovo XClarity Administrator potrebbe visualizzare uno stato di alimentazione non corretto per il server.

Per risolvere questo problema, completare una delle seguenti procedure:
- Verificare che i server bare metal siano spenti.
- Per XClarity Administrator v1.2.2 o versioni successive, avviare il server con la configurazione BIOS/UEFI (F1) (vedere Accensione e spegnimento di un server nella documentazione online di XClarity Administrator).

Capitolo 6. Problemi di installazione, rimozione, aggiornamento e migrazione dei dati

Utilizzare queste informazioni per risolvere problemi di installazione, rimozione, aggiornamento e migrazione dei dati.

L'uscita video non funziona quando si installa XClarity Administrator in Red Hat KVM

Quando si installa l'appliance virtuale Lenovo XClarity Administrator mediante l'interfaccia utente di Red Hat KVM, l'uscita video potrebbe non funzionare tramite la console, causando una schermata nera sulla console all'accensione della macchina virtuale XClarity Administrator, invece di visualizzare il banner della macchina virtuale con informazioni sull'IP di XClarity Administrator.

Per visualizzare l'uscita video tramite la console, verificare che il dispositivo video sia impostato su **Cirrus** aprendo la schermata dei dettagli dell'hardware virtuale di XClarity Administrator e facendo clic su **Video** nel riquadro di navigazione sinistro. Per impostazione predefinita, l'interfaccia utente RedHat KVM configura il dispositivo video su QXL.

Le modifiche apportate all'adattatore non vengono riconosciute

Dopo aver rimosso, sostituito o configurato gli adattatori, Lenovo XClarity Administrator non riconosce le modifiche.

Riavviare il dispositivo per consentire al controller di gestione della scheda di base (BMC) di riconoscere le modifiche. Per ulteriori informazioni, consultare la sezione Documentazione online di System x.

Durante la configurazione iniziale non è possibile avviare la procedura guidata di configurazione iniziale in un browser Web

Utilizzare queste informazioni per risolvere i problemi di configurazione iniziale di Lenovo XClarity Administrator.

1. Accertarsi che il sistema host fisico soddisfi i requisiti minimi (vedere Sistemi host supportati nella documentazione online di XClarity Administrator).
2. Accertarsi che si stia utilizzando un sistema virtuale supportato che soddisfi i requisiti di sistema minimi (vedere Sistemi host supportati nella documentazione online di XClarity Administrator).
3. Verificare che la versione del browser Web sia compatibile con XClarity Administrator. Per un elenco dei browser Web supportati, vedere Accesso all'interfaccia Web di XClarity Administrator nella documentazione online di XClarity Administrator.
4. Per impostazione predefinita, per le configurazioni di rete è abilitato il protocollo DHCP. Verificare che sia stato assegnato un indirizzo IP valido eseguendo il login alla macchina virtuale in locale, quindi il comando `ifconfig`. Se si utilizza una configurazione statica, accertarsi di seguire le operazioni riportate di seguito per configurare correttamente l'installazione. Per ulteriori informazioni, vedere Installazione di XClarity Administrator in ambienti basati su VMware ESXi nella documentazione online di XClarity Administrator.

© Copyright Lenovo 2015, 2025

Errore imprevisto della distribuzione di Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi di configurazione iniziale di Lenovo XClarity Administrator.

1. Cercare eventuali eventi correlati alla distribuzione nel relativo log e risolverli. Per ulteriori informazioni sul log eventi, vedere Utilizzo degli eventi nella documentazione online di XClarity Administrator.
2. Accertarsi che il sistema host fisico soddisfi i requisiti minimi.
3. Accertarsi che il sistema o il sistema virtuale soddisfi i requisiti minimi.
4. Accertarsi di utilizzare un gestore di macchine virtuali supportato.

Per ulteriori informazioni sui requisiti, vedere Sistemi host supportati nella documentazione online di XClarity Administrator.

Aggiornamento di Lenovo XClarity Administratornon riuscito

Utilizzare queste informazioni per risolvere i problemi di aggiornamento di Lenovo XClarity Administrator.

1. Accertarsi di aver installato eventuali aggiornamenti essenziali.
2. Accertarsi di disporre delle autorizzazioni utente per installare gli aggiornamenti.

Per ulteriori informazioni sull'aggiornamento di XClarity Administrator, vedere Aggiornamento del server di gestione di XClarity Administrator nella documentazione online di XClarity Administrator.

Capitolo 7. Problemi di connettività

Utilizzare queste informazioni per risolvere problemi di connettività.

Impossibile accedere a Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi di connettività a Lenovo XClarity Administrator.

Se si è verificato un arresto imprevisto del sistema operativo host, ripristinare XClarity Administrator dall'ultimo backup. Per informazioni sul backup e sul ripristino di XClarity Administrator, vedere Backup e ripristino di XClarity Administrator nella documentazione online di XClarity Administrator.

Impossibile connettersi a Lenovo XClarity Administrator utilizzando il browser Safari

Utilizzare queste informazioni per risolvere i problemi di connettività a XClarity Administrator utilizzando il browser Safari.

Durante il tentativo di connessione all'interfaccia Web di XClarity Administrator utilizzando un browser Web Safari, verrà visualizzato un elenco dei certificati client associati all'account utente personale. La scelta di uno di questi certificati potrebbe generare un errore di "connessione non riuscita". Questo problema potrebbe verificarsi poiché il browser Web Safari tenta di inviare un certificato client a XClarity Administrator, ma il certificato client non è valido per il server XClarity Administrator. Per risolvere il problema, eliminare il certificato client e tentare di connettersi nuovamente all'interfaccia Web di XClarity Administrator. Per ulteriori informazioni su questo problema in caso di utilizzo del browser Safari, vedere la Pagina Web dei problemi di certificato dei client Safari.

Impossibile eseguire il login

Utilizzare queste informazioni per risolvere i problemi quando si esegue il login a un modulo CMM e al controller di gestione della scheda di base di Lenovo XClarity Administrator.

Impossibile eseguire il login a Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi durante il login a Lenovo XClarity Administrator.

1. Verificare che la password sia corretta e che BLOC MAIUSC e BLOC NUM non siano attivati.
2. Accertarsi che l'account utente non sia bloccato. Se è bloccato, chiedere a un supervisore di sbloccarlo (vedere Sblocco di un utente nella documentazione online di XClarity Administrator).
3. Accertarsi che l'account utente non sia disabilitato. Se è disabilitato, chiedere a un supervisore di abilitarlo (vedere Abilitazione o disabilitazione di un utente nella documentazione online di XClarity Administrator).
4. In caso di utilizzo di un server di autenticazione esterna:
   a. Accertarsi che i gruppi di ruoli corretti siano configurati in XClarity Administrator. Per informazioni sui gruppi di ruoli, vedere Creazione di un gruppo di ruoli nella documentazione online di Lenovo XClarity Administrator.
   b. Verificare che gli account utente siano definiti come membri di uno dei gruppi di ruoli nel server di autenticazione esterna.

© Copyright Lenovo 2015, 2025

c. Se è stata modificata la password per l'account client utilizzato per collegare XClarity Administrator al server di autenticazione esterna, accertarsi di aggiornare la nuova password anche nell'interfaccia Web di XClarity Administrator:
   1) Eseguire il log in a XClarity Administrator utilizzando il nome client e la password attualmente definiti in XClarity Administrator (vedere Configurazione di un server di autenticazione esterna nella documentazione online di XClarity Administrator).
   2) Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
   3) Fare clic su **Client LDAP** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni client LDAP.
   4) Aggiornare la password nel campo **Password client** e fare clic su **Applica**.

   Se l'account client è bloccato a causa di troppi tentativi di login non riusciti in seguito alla modifica della password nel server di autenticazione esterna, sbloccare l'account direttamente nel server di autenticazione esterna o attendere la scadenza del periodo di blocco e tentare di modificare la password in XClarity Administrator.

d. Se la password per l'account client utilizzato per collegare XClarity Administrator al server di autenticazione esterna è scaduta, attenersi alla procedura descritta di seguito per sbloccare l'account e modificare la password in XClarity Administrator.
   1) Sbloccare l'account client, quindi modificare la password client nel server di autenticazione esterna.
   2) Eseguire il log in a XClarity Administrator utilizzando il nome client e la password attualmente definiti in XClarity Administrator (vedere Configurazione di un server di autenticazione esterna nella documentazione online di XClarity Administrator).
   3) Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
   4) Fare clic su **Client LDAP** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni client LDAP.
   5) Aggiornare la password nel campo **Password client** e fare clic su **Applica**.

5. Se si è verificato un arresto imprevisto del sistema operativo host e si riceve un errore di autenticazione, ripristinare XClarity Administrator dall'ultimo backup. Per informazioni sul backup e sul ripristino di XClarity Administrator, vedere Backup e ripristino di XClarity Administrator nella documentazione online di XClarity Administrator.

Password per il ripristino locale o un utente supervisore dimenticata

account supervisore o se un altro account supervisore non esiste, è possibile reimpostare la password per un utente locale con autorità **lxc-recovery** o **lxc-supervisor** montando un'immagine ISO che contiene un file di configurazione con la nuova password.

Prima di iniziare

Attenzione: Questa procedura non è appropriata per XClarity Administrator v3.3.x e v3.4.x. Se si utilizza una di queste versioni, contattare il supporto Lenovo e richiedere assistenza per ripristinare l'accesso a XClarity Administrator.

Per reimpostare la password con questo metodo, è necessario disporre dell'accesso al sistema host XClarity Administrator.

Il nome utente che verrà reimpostato deve disporre dell'autorità **lxc-recovery** o **lxc-supervisor**.

La password deve rispettare le stesse regole di convalida applicate da XClarity Administrator

Una volta reimpostata la password, l'utente non dovrà necessariamente modificarla al primo accesso

Procedura

Per creare e montare l'immagine ISO, completare la seguente procedura.

1. Spegnere la macchina virtuale.
2. Creare un file denominato `passwordreset.properties` contenente i seguenti parametri.
   ```
   user=
   password=
   ```
   È possibile utilizzare il comando echo per creare il file, ad esempio:
   ```
   ECHO user=admin > ./ passwordreset.properties
   ECHO password=New_PasswOrd >> ./ passwordreset.properties
   ```
3. Creare un'immagine ISO contenente il file passwordreset.properties.

   Per creare un'immagine ISO in Windows, utilizzare un software ISO qualsiasi. In Linux, utilizzare il comando `mkisofs`, ad esempio

   ```
   mkisofs -V passreset -J -o ./passreset.iso ./passwordreset.properties
   ```

   dove **-V** è l'etichetta del volume, **-J** è il formato Joliet, **-o** è il nome del file di output e **/ passwordreset. properties** è il file da includere nell'immagine ISO.
4. Caricare l'immagine ISO in una posizione idonea esplorando l'archivio dati.
5. Montare l'immagine ISO nella macchina virtuale.
   - **Per Citrix**:
     a. Montare l'immagine ISO di configurazione come unità CD fisica nella macchina virtuale.
     b. Da Citrix, selezionare la macchina virtuale XClarity Administrator.
     c. Selezionare la scheda **Console**.
     d. Selezionare il CD fisico dall'elenco delle unità.
   - **Per gli host Nutanix AHV:**
     a. Fare clic sul menu **Impostazioni** (⚙) e quindi su **Configurazione immagini** per visualizzare la finestra di dialogo "Configurazione immagini".
     b. Caricare l'immagine `eth0_config.iso`.
        1) Dalla finestra di dialogo Configurazione immagini, fare clic su **Carica immagine** per visualizzare nuovamente la finestra di dialogo Crea immagine.
        2) Specificare un nome per l'immagine ISO.
        3) Selezionare "ISO" come tipo di immagine.
        4) Selezionare **Carica un file**, fare clic su **Scegli file**, quindi selezionare l'immagine `eth0_config.iso`.
        5) Fare clic su **Salva** per caricare il file.
        6) Fare clic su **Chiudi** per chiudere la finestra di dialogo Configurazione immagini.
     c. Prima di continuare con le operazioni di configurazione, attendere il completamento dei processi di caricamento. Il cerchio di stato nel menu indica quando i processi sono completi.
     d. Aggiungere un disco per l'immagine `eth0_config.iso`.
        1) Dalla macchina virtuale, fare clic su **Aggiorna** dalla barra dei menu inferiore.
        2) Fare clic sull'icona **Modifica** del disco CDROM per visualizzare la finestra di dialogo Modifica disco.
        3) Selezionare **Clona** da servizio immagini per le operazioni.
        4) Selezionare l'immagine ISO creata in precedenza dall'elenco di immagini.
        5) Fare clic su **Aggiorna**.

6) Fare clic su **Salva**.

- **Per gli host RedHat KVM:**
  a. Da Virtual Machine Manager, selezionare la macchina virtuale e quindi fare clic su **Aggiungi Hardware** per visualizzare la finestra di dialogo "Aggiungi nuovo hardware virtuale".
  b. Fare clic sulla scheda **Storage**.
  c. Selezionare **Seleziona lo storage gestito o di altro tipo esistente**, fare clic su **Sfoglia** e selezionare l'immagine `eth0_config.iso`.
  d. Selezionare **VirtIO** per il tipo di dispositivo.

     Nota: Per XClarity Administrator 1.4.0 e versioni precedenti, selezionare **IDE** per il bus del disco.
  e. Selezionare **Nessuno** per la modalità di cache.
  f. Fare clic su **Fine**.
- **Per gli host VMware ESXi:**

  Il file ISO deve trovarsi nell'archivio dati dell'host ESXi, in modo da poterlo montare come unità CD/DVD nella macchina virtuale di XClarity Administrator.
  a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Modifica impostazioni**.
  b. Fare clic su **Aggiungi** per visualizzare la procedura guidata Aggiungi hardware.
  c. Fare clic su **Unità CD/DVD** e su **Avanti**.
  d. Selezionare **Usa immagine ISO** e fare clic su **Avanti**.
  e. Selezionare l'immagine ISO e fare clic su **Avanti**.
  f. Selezionare il nodo del dispositivo virtuale e fare clic su **Avanti**.
  g. Fare clic su **Fine**.
- **Per gli host Windows Hyper-V:**

  Importante: Prima di montare l'immagine ISO, è necessario spegnere la macchina virtuale.
  a. Nella finestra Hyper-V Manager fare clic con il pulsante destro del mouse sull'appliance virtuale e scegliere **Connetti** per visualizzare la finestra Connessione macchina virtuale.
  b. Fare clic su **Supporti → Unità DVD → Inserisci disco**.
  c. Selezionare l'immagine ISO e fare clic su **Apri**.

6. Accendere la macchina virtuale ed eseguire il login all'interfaccia Web di XClarity Administrator utilizzando il nome utente e la password specificata nel file `passwordreset.properties` (vedere Accesso all'interfaccia Web di XClarity Administrator nella documentazione online di XClarity Administrator).
7. Smontare l'unità ed eliminare l'immagine ISO.
   - Per Citrix
     a. Nell'hypervisor Citrix selezionare la macchina virtuale XClarity Administrator.
     b. Selezionare la scheda **Console**.
     c. Cancellare il CD fisico associato all'immagine ISO di configurazione dall'elenco dei driver.
   - **Per gli host Nutanix AHV:**
     a. Dalla macchina virtuale, fare clic su **Aggiorna** dalla barra dei menu inferiore.
     b. Fare clic sull'icona **Modifica** del disco CDROM per visualizzare la finestra di dialogo Modifica disco.
     c. Fare clic sull'icona **Espelli**.
     d. Fare clic su **Salva**.
   - **Per gli host VMware ESXi:**

a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Modifica impostazioni**.
b. Selezionare l'unità montata dall'elenco hardware e fare clic su **Rimuovi**.
c. Fare clic su **OK**. L'unità è ora scollegata.
d. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere nuovamente **Modifica impostazioni**.
e. Selezionare l'unità dall'elenco hardware e deselezionare la casella di controllo **Connetti all'accensione**.
f. Fare clic su **OK**.
g. Eliminare l'immagine ISO dall'archivio dati.

- **Per gli host Windows Hyper-V:**
  a. Nella finestra Hyper-V Manager fare clic con il pulsante destro del mouse sull'appliance virtuale e scegliere **Connetti** per visualizzare la finestra Connessione macchina virtuale.
  b. Fare clic su **Supporti → Unità DVD → Espelli** *iso_image_name***.iso**.
  c. Eliminare l'immagine ISO dall'archivio dati.

Impossibile eseguire il login direttamente al modulo CMM gestito

Utilizzare queste informazioni per risolvere i problemi quando si esegue il login direttamente a un modulo CMM gestito.

1. Verificare che la password sia corretta e che BLOC MAIUSC e BLOC NUM non siano attivati.
2. Verificare che le credenziali corrispondano a quelle memorizzate in Lenovo XClarity Administrator. Se il modulo CMM è gestito da XClarity Administrator, non sarà possibile eseguire il login con gli account CMM locali. Per ulteriori informazioni sulla gestione centralizzata degli utenti in XClarity Administrator, vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator.

Impossibile eseguire il login direttamente al controller di gestione

Utilizzare queste informazioni per risolvere i problemi quando si esegue il login direttamente a un controller di gestione.

1. Verificare che la password sia corretta e che BLOC MAIUSC e BLOC NUM non siano attivati.
2. Verificare che le credenziali corrispondano a quelle memorizzate in Lenovo XClarity Administrator.
3. Verificare che la versione del controller di gestione sia compatibile con XClarity Administrator.
4. Verificare che solo un server XClarity Administrator gestisca il controller di gestione.

Impossibile eseguire il login ai server Flex Power System gestiti

Utilizzare queste informazioni per risolvere i problemi quando si esegue il login direttamente ai server Flex Power System gestiti - Lenovo XClarity Administrator

Se si dispone di uno chassis contenente server Flex System e Flex Power System, potrebbe non essere possibile eseguire il login direttamente ai server Flex Power System a causa di errori di autenticazione.

Se lo chassis è gestito da XClarity Administrator, il modulo CMM viene inserito nella gestione centrale degli utenti. In altre parole, gli account utente definiti nel server di autenticazione interna o esterna consentono inoltre di eseguire il login al modulo CMM (Chassis Management Module) e gli account utente CMM locali sono disabilitati.

Per eseguire il login all'interfaccia Web del controller di gestione di un server Flex Power System gestito, utilizzare l'account RECOVERY_ID creato quando lo chassis era gestito da XClarity Administrator. Eseguire il login al modulo CMM con questo account e modificare la password. La password deve essere modificata al primo accesso. Dopo aver modificato la password, sarà possibile eseguire il login all'interfaccia Web del controller di gestione del nodo Power Systems con l'account RECOVERY_ID.

Se si desidera gestire un nodo Flex Power System da una console HMC (Hardware Management Console), attenersi alla procedura descritta di seguito.

1. Eseguire il login all'interfaccia della CLI di gestione mediante SSH.
2. Eseguire i seguenti comandi per configurare il metodo di autenticazione utente nel modulo CMM su **Prima locale, poi autenticazione esterna**, quindi eliminare e ricreare l'account USERID.
```
env -T mm[p]
accseccfg -am localldap
users -n USERID -clear
users -add -n USERID -p <password> -g Supervisor -ms 0
```

Perdita improvvisa di connettività a un dispositivo

Utilizzare queste informazioni per risolvere i problemi di connettività a un singolo dispositivo

1. Se il dispositivo che utilizza la credenziale memorizzata è offline, verificare che la credenziale memorizzata non sia scaduta o non valida. Se la credenziale è scaduta o non valida, completare le seguenti operazioni:
   a. Dalla pagina "Tutti i dispositivi", selezionare il dispositivo da risolvere.
   b. Fare clic su **Tutte le azioni → Sicurezza → Risolvi credenziali memorizzate**.
   c. Modificare la password per la credenziale memorizzata o selezionare un'altra credenziale memorizzata da utilizzare per il dispositivo gestito.
2. Cercare eventuali eventi di rete per il dispositivo nel relativo log e risolverli. Per ulteriori informazioni sul log eventi, vedere Utilizzo degli eventi nella documentazione online di Lenovo XClarity Administrator.
3. Accertarsi che l'hardware di rete funzioni correttamente per il percorso di connessione al dispositivo.
4. Accertarsi che lo switch e le porte firewall corretti siano abilitati per il dispositivo. Per informazioni sulle porte richieste, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
5. Accertarsi che sia presente una configurazione di rete valida nel dispositivo eseguendo il login e verificando che l'indirizzo IP sia valido per la rete. È inoltre possibile effettuare il ping del dispositivo per testare se è visibile nella rete.
6. Tentare di eseguire il login direttamente al dispositivo.

Capitolo 8. Problemi di configurazione di Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi di configurazione di Lenovo XClarity Administrator.

Problemi di configurazione del server LDAP esterno

Utilizzare queste informazioni per risolvere i problemi durante la configurazione di un server di autenticazione esterna.

1. Accertarsi che il nome distinto radice sia corretto.
2. Verificare che l'account utente Lenovo XClarity Administrator sia membro almeno di un gruppo di ruoli. Per informazioni sui gruppi di ruoli, vedere Creazione di un gruppo di ruoli nella documentazione online di XClarity Administrator.
3. Verificare che il gruppo di ruoli XClarity Administrator corrisponda ad almeno un gruppo di ruoli nel server LDAP.
4. Se si utilizzano indirizzi server preconfigurati, accertarsi che l'indirizzo IP e il numero di porta del server siano corretti.
5. Verificare che le impostazioni di configurazione DNS siano corrette.
6. Se si utilizza DNS per rilevare i server, accertarsi che il nome di dominio e il nome della foresta siano corretti.
7. Accertarsi che il nome distinto e la password del client siano corretti

Per informazioni sulla configurazione di un server di autenticazione esterna, vedere Configurazione di un server di autenticazione esterna nella documentazione online di XClarity Administrator.

Non si dispone dell'autorizzazione necessaria a configurare i server

Utilizzare queste informazioni per risolvere i problemi durante la configurazione dei server gestiti.

1. Accertarsi di aver eseguito il login a un account utente che appartiene a un gruppo di ruoli di supervisore o amministratore. Per informazioni sui ruoli utente, vedere Creazione di un gruppo di ruoli nella documentazione online di Lenovo XClarity Administrator.
2. Per aggiornare l'autorità, contattare l'amministratore di sistema.

Problemi di attivazione di Features on Demand

Utilizzare queste informazioni per risolvere i problemi di attivazione delle funzioni.

Accertarsi di seguire le istruzioni relative allo strumento utilizzato per applicare la chiave Features on Demand (FoD). Per ulteriori informazioni sulle chiavi FoD, vedere Visualizzazione delle chiavi FoD (Feature on Demand) nella documentazione online di Lenovo XClarity Administrator.

Avviso di VMware di mancato supporto del driver VMXNET 3

Potrebbe essere visualizzato un avviso di mancato supporto del driver VMXNET 3 quando si installa Lenovo XClarity Administrator, si modificano le impostazioni della macchina virtuale dell'appliance XClarity Administrator, si esegue la funzione vMotion di XClarity Administrator o all'interno dell'infrastruttura di gestione e monitoraggio associata di VMware.

© Copyright Lenovo 2015, 2025

L'appliance XClarity Administrator include il driver VMXNET 3. È possibile ignorare eventuali errori VMware relativi al mancato supporto del driver.

Capitolo 9. Problemi di prestazioni

Utilizzare queste informazioni per risolvere i problemi di prestazioni.

Problemi di prestazioni di Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi di prestazioni di Lenovo XClarity Administrator.

Se si dispone di un ambiente con un numero elevato di dispositivi e di numerose sessioni utente simultanee che causano la riduzione delle prestazioni del sistema, diminuire il numero di sessioni utente simultanee dall'interfaccia Web di XClarity Administrator oppure aumentare le risorse virtuali della CPU allocate all'appliance virtuale.

Accertarsi che le risorse disponibili sulla macchina virtuale (memoria, dimensione del disco, processore) consentano di gestire il numero di dispositivi desiderato. Per ulteriori informazioni sui requisiti delle macchine virtuali, vedere Sistemi host supportati nella documentazione online di XClarity Administrator.

Per suggerimenti e ulteriori considerazioni sulle prestazioni, vedere XClarity Administrator: guida alle prestazioni (white paper).

Prestazioni di rete scadenti o lente

Utilizzare queste informazioni per risolvere i problemi di prestazioni di rete scadenti o lente.

1. Accertarsi che non siano in esecuzione operazioni di rete significative, quali il rilevamento di sistemi, la distribuzione di sistemi operativi o l'esecuzione di aggiornamenti firmware.
2. Accertarsi che il resto della rete sia operativo alla capacità nominale.
3. In caso di implementazione di Qualità del servizio (QoS), accertarsi che sia configurato per consentire la connettività ottimale a Lenovo XClarity Administrator.
4. Accertarsi che la topologia di rete sia ottimizzata per la connettività e le prestazioni di XClarity Administrator.

© Copyright Lenovo 2015, 2025

Capitolo 10. Problemi di sicurezza

Utilizzare queste informazioni per risolvere i problemi di sicurezza, tra cui quelli relativi all'autenticazione e alla gestione degli utenti.

Il certificato SSL non viene ritenuto attendibile

La catena di certificati potrebbe contenere una firma autofirmata o non provenire da un'autorità di certificazione nota.

Porte 443, 3888, 9090, 50636, 50637
Ogni istanza di Lenovo XClarity Administrator dispone di un'autorità di certificazione univoca, generata internamente. Per impostazione predefinita, queste porte (utilizzate per la comunicazione tra l'utente e l'appliance virtuale o tra i dispositivi gestiti e l'appliance virtuale), utilizzano un certificato firmato dall'autorità di certificazione. Se il certificato SSL non viene ritenuto attendibile, generare e distribuire un certificato del server con firma esterna personalizzato in XClarity Administrator. Per ulteriori informazioni, vedere Distribuzione dei certificati personalizzati dei server a XClarity Administrator nella documentazione online di XClarity Administrator.

Porta 8443
Ogni istanza XClarity Administrator dispone di un'autorità di certificazione univoca, utilizzata solo per la distribuzione del sistema operativo. L'autorità di certificazione firma un certificato che viene utilizzato per il server di destinazione sulla porta 8443. Quando viene avviata la distribuzione del sistema operativo, il certificato CA viene incluso nell'immagine del sistema operativo che verrà inviata al server di destinazione. Durante il processo di distribuzione, il server si collega alla porta 8443 per verificare il certificato fornito dalla porta 8443 durante l'handshake, poiché in possesso del certificato CA.

Convalida della certificazione del server non riuscita

Utilizzare queste informazioni quando si tenta di installare un certificato server in Lenovo XClarity Administrator e la convalida ha esito negativo.

Informazioni su questa attività

La convalida della certificazione del server potrebbe avere esito negativo se XClarity Administrator tenta di:

- Connettersi a dispositivi gestiti mediante CIM-XML su HTTPS.
- Raggiungere un server di autenticazione esterna mediante il protocollo LDAP sicuro (se è stata configurata una connessione LDAP sicura).
- Raggiungere un provider di identità SAML esterno mediante una connessione sicura (se è stata configurata una connessione SAML).
- Connettersi ai file server remoti importare le immagini del sistema operativo (se è stato configurato un server di immagini HTTPS).
- Connettersi a Lenovo per ottenere informazioni sullo stato di garanzia.
- Connettersi al server di notifiche push Apple e Google (se le notifiche push Lenovo XClarity Mobile sono abilitate per un dispositivo iOS o Android).

Procedura

Per risolvere il problema, completare le seguenti operazioni.

© Copyright Lenovo 2015, 2025

- Accertarsi che il certificato o il relativo certificato di firma sia presente nell'archivio attendibile Certificati sicuri o Certificati servizi esterni in XClarity Administrator. Per ulteriori informazioni sui certificati attendibili e sui certificati di servizi esterni, vedere Utilizzo dei certificati di sicurezza nella documentazione online di XClarity Administrator.
- Accertarsi che il certificato non sia stato revocato (vedere Aggiunta e sostituzione di un elenco di revoche di certificati nella documentazione online di XClarity Administrator).
- Accertarsi che l'indirizzo IP o il nome host del server corrisponda a uno dei nomi alternativi o al nome comune dell'oggetto (se SAN non è presente) nel certificato.
- Accertarsi che la data odierna sia compresa tra le date "Non valido prima" e "Non valido dopo" nel certificato.
- Accertarsi che il certificato venga firmato mediante un algoritmo supportato, SHA1 o più complesso in modalità legacy oppure SHA256 o più complesso in modalità strict NIST (vedere Impostazione della modalità crittografica e dei protocolli di comunicazione nella documentazione online di XClarity Administrator).

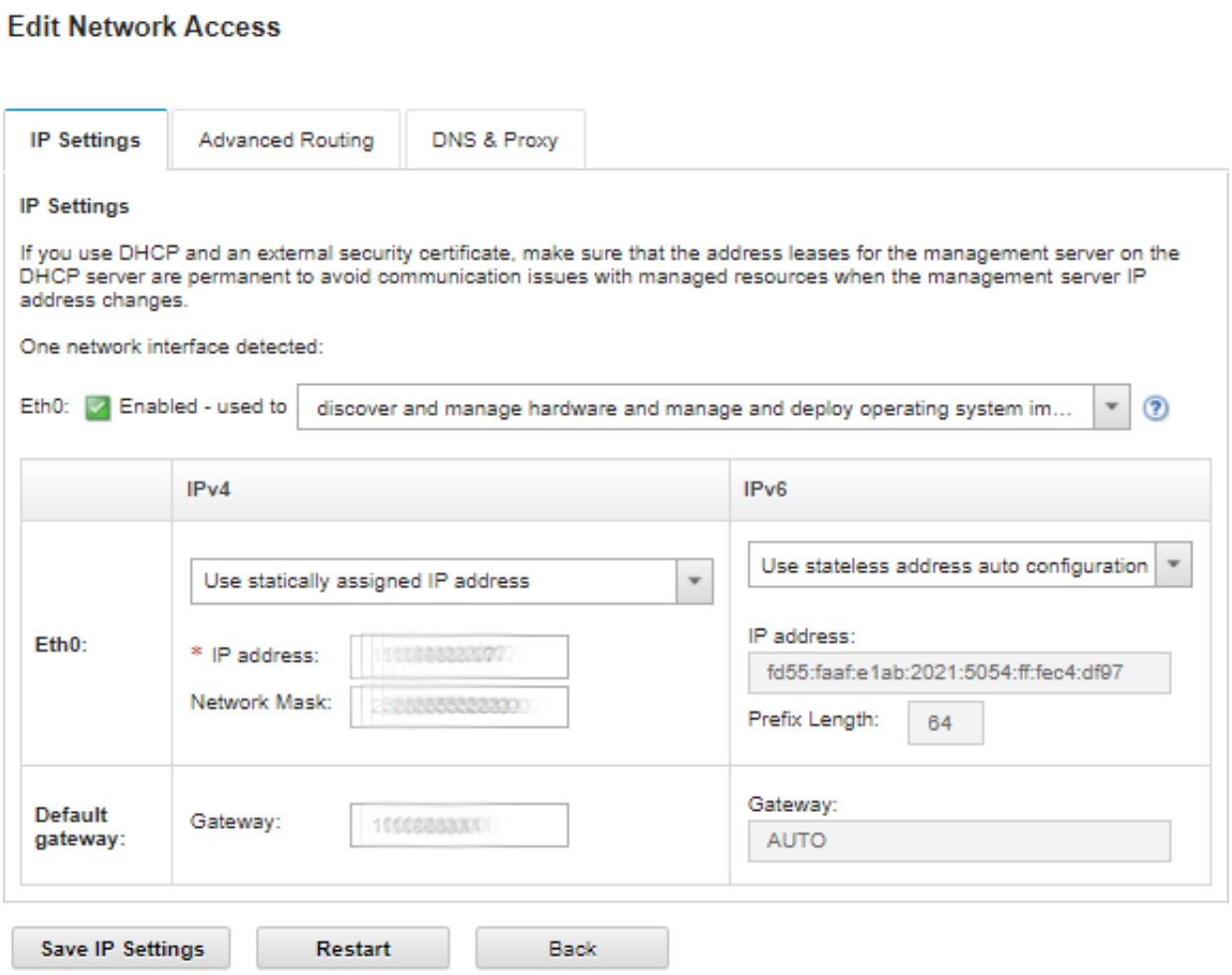
Vulnerabilità Samba e Apache

Durante la distribuzione del sistema operativo e l'aggiornamento dei driver di dispositivo del sistema operativo, Lenovo XClarity Administrator utilizza i server Samba e Apache come condivisione remota di sola lettura. Se non si desidera utilizzare XClarity Administrator per gestire i sistemi operativi, è possibile disabilitare i server Samba e Apache configurando il ruolo della rete XClarity Administrator per rilevare e gestire solo l'hardware.

Procedura

Per disabilitare i server Samba e Apache, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Accesso alla rete**. Vengono visualizzate le impostazioni di rete attualmente definite.
2. Fare clic su **Modifica accesso alla rete** per visualizzare la pagina "Modifica accesso alla rete".



3. Selezionare l'opzione **rileva e gestisci solo l'hardware** per l'interfaccia di rete.
4. Fare clic su **Salva impostazioni IP**.
5. Fare clic su **Riavvia** per riavviare il server di gestione.

Capitolo 11. Risoluzione dei problemi di backup e ripristino

Utilizzare queste informazioni per risolvere i problemi di backup e ripristino.

Il processo di backup sembra bloccarsi durante il riavvio del server di gestione

La creazione di un backup di Lenovo XClarity Administrator potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

Procedura

Se il processo di backup sembra bloccarsi, attenersi alla procedura descritta di seguito.

- Se il pulsante **Annulla** viene visualizzato, è possibile annullare il processo di backup.
- Se il pulsante **Annulla** non viene visualizzato, aprire una nuova scheda per verificare se il pulsante **Annulla** viene visualizzato.
- Se il problema persiste, riavviare la macchina virtuale.

Nota: Se si annulla il processo di backup o si riavvia la macchina virtuale, potrebbe non essere possibile creare il backup.

La finestra XClarity Administrator è vuota dopo averla aggiornata durante il backup

Lenovo XClarity Administrator rimarrà inattivo durante la procedura per prevenire la modifica dei dati. Se si aggiorna o si chiude la finestra XClarity Administrator prima che il processo di backup sia stato completato e il server di gestione viene riavviato, la finestra XClarity Administrator potrebbe sembrare vuota se il server di gestione è ancora in modalità di disattivazione.

Procedura

Per risolvere questo problema, completare le seguenti operazioni.

1. Aggiornare la pagina periodicamente per verificare se viene caricata.
2. Se la finestra resta vuota per molto tempo, riavviare la macchina virtuale.
3. Se ancora non si carica, eliminare manualmente il file `/opt/lenovo/lxca/bin/QUIESCE_MODE_FLAG`.

   Nota: Questa operazione richiede l'accesso alla radice. Prima di eseguire questa operazione, contattare il supporto.
4. Riavviare la macchina virtuale XClarity Administrator.

© Copyright Lenovo 2015, 2025

Capitolo 12. Problemi di monitoraggio e inoltro di eventi

Utilizzare queste informazioni per risolvere problemi di monitoraggio e inoltro di eventi.

Gli eventi non vengono inoltrati

Utilizzare queste informazioni per risolvere i problemi durante l'inoltro di eventi.

- Se per il server d'inoltro degli eventi viene creata una pianificazione, verranno inoltrati solo gli eventi che si verificheranno durante l'orario pianificato. Accertarsi che l'orario pianificato non sia trascorso.
- Per i servizi Web basati su e-mail:
  - Se per il server d'inoltro degli eventi viene selezionato un tipo di connessione sicura, Lenovo XClarity Administrator tenta di scaricare e importare il certificato del server SMTP nel proprio archivio attendibile. All'utente verrà richiesto di accettare l'aggiunta di questo certificato nell'archivio attendibile. In caso di esito negativo, non sarà possibile stabilire la connessione al server SMTP.

    Per risolvere il problema, importare manualmente il certificato nell'archivio attendibile di XClarity Administrator facendo clic su **Amministrazione → Sicurezza → Certificati attendibili** e sull'icona **Crea** ( ).
  - Verificare se il server SMTP accetta solo i messaggi e-mail inviati da un utente registrato. In questo caso, l'indirizzo del mittente predefinito (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) verrà rifiutato. Per risolvere questo problema, specificare almeno un nome di dominio nel campo **Indirizzo di provenienza** nel server d'inoltro degli eventi.
  - Se si utilizza l'autenticazione OAUTH2, verificare che il token di sicurezza non sia scaduto. Se è scaduto, utilizzare lo script Python oauth2.py e il token di aggiornamento per generare un nuovo token di sicurezza. Aggiornare quindi il server d'inoltro degli eventi in XClarity Administrator con il nuovo token di sicurezza. Per ulteriori informazioni, vedere Configurazione dell'inoltro eventi a un servizio SMTP Gmail.

© Copyright Lenovo 2015, 2025

Capitolo 13. Problemi relativi alla gestione dei dispositivi

Utilizzare queste informazioni per risolvere i problemi di funzionamento e gestione dei dispositivi.

Impossibile cancellare in modo sicuro i dati dell'unità sulle unità bloccate

Utilizzare queste informazioni per risolvere i problemi di cancellazione sicura delle unità disco SATA con errore indicante che i dischi sono bloccati e non possono essere cancellati.

Per impostazione predefinita, le unità disco SATA integrate sono bloccate. Se il server dispone di un'unità bloccata, Lenovo XClarity Administrator sblocca temporaneamente tale unità e avvia l'aggiornamento bare metal (BMU, Bare Metal Update) per cancellarla. Quando l'aggiornamento BMU di XClarity Administrator si chiude e il server si avvia sul sistema operativo, l'unità viene nuovamente bloccata automaticamente.

Quando un server è gestito in XClarity Administrator tramite la modalità di *autenticazione gestita*, XClarity Administrator crea l'account LDAP SYSMGR_xxx per gestire e monitorare il server anziché le credenziali locali (vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator). L'account LDAP SYSMGR_xxx non dispone di un privilegio IPMI, pertanto XClarity Administrator non può sbloccare il disco e di conseguenza l'operazione di cancellazione sicura sul server non avverrà.

Per risolvere il problema, gestire il server utilizzando la modalità di *autenticazione locale* e tentare di cancellare in modo sicuro le unità.

Impossibile cancellare in modo sicuro i volumi SDD SATA quando sono collegati a controller RAID Marvell

Utilizzare queste informazioni per risolvere i problemi di mancata cancellazione sicura su unità SDD SATA con volumi collegati a controller RAID Marvell.

Non è possibile cancellare in modo sicuro i volumi SDD SATA collegati ai controller RAID SATA. Tenere invece in considerazione i consigli che seguono.

- Per le unità SSD SATA da 7 mm, collegarsi ai controller RAID Broadcom per eseguire una cancellazione sicura.
- Per le unità SSD SATA M.2, collegarsi ai controller non RAID Marvell (come il kit di abilitazione a 2 vani SATA/NVMe M.2 per ThinkSystem) per eseguire un'operazione di cancellazione sicura.

Si verifica un timeout interno (9 secondi) nel firmware RAID Marvell. Se l'unità SSD non risponde in tempo al comando (non completa la cancellazione), il firmware RAID Marvell reimposta l'unità SDD, l'unità SDD si blocca e la cancellazione sicura non riesce. Per sbloccare l'unità SDD , eseguire il comando indicato sotto.

```
hdparm --user-master u --security-unlock user123 %diskName%
```

I dati di inventario non vengono aggiornati dopo l'aggiunta o la sostituzione di schede

Per i dispositivi basati su AMD1P e TSM, Lenovo XClarity Administrator potrebbe non visualizzare dati di inventario corretti, come FRU e firmware, per le schede PCIe appena inserite.

© Copyright Lenovo 2015, 2025

Dopo aver modificato una scheda PCIe, è necessario riavviare il dispositivo gestito e attendere alcuni minuti perché il controller di gestione della scheda di base aggiorni l'inventario.

XClarity Administrator recupera automaticamente i dati di inventario dai dispositivi gestiti ogni 24 ore. È possibile attendere la successiva raccolta dell'inventario oppure è possibile raccogliere manualmente i dati di inventario selezionando il server nella pagina Server e facendo quindi clic su **Azioni → Inventario → Aggiorna inventario**.

Capitolo 14. Problemi di configurazione dei server

Utilizzare queste informazioni per risolvere i problemi con profili e pattern server.

Errore durante la creazione di un pattern da un server esistente

Utilizzare queste informazioni per risolvere i problemi durante la creazione di pattern server da un server gestito esistente.

1. Accertarsi che lo stato del server non sia offline. Per ulteriori informazioni sui pattern server, vedere Creazione di un pattern server nella documentazione online di Lenovo XClarity Administrator.
2. Ripetere l'operazione.

Errore di attivazione durante la distribuzione di un pattern in un dispositivo

Un errore di attivazione indica che si è verificato un problema durante la distribuzione del pattern server in un dispositivo gestito. Un errore di attivazione potrebbe verificarsi per diversi motivi. Utilizzare queste informazioni per risolvere questi tipi di problemi.

Esaminare i dettagli del processo dalla relativa pagina individuando il processo di attivazione del profilo server con stato "Arrestato con errori" e selezionandolo. Per identificare il problema, esaminare i messaggi di errore.

- Problemi di connettività o instradamento di rete tra Lenovo XClarity Administrator e il dispositivo gestito.

  Queste problemi potrebbero essere rappresentati nei messaggi del processo come errori LDAP. Ciò indica che si è verificato un problema relativo al dispositivo che si connette all'appliance virtuale su una delle interfacce di rete configurate.

  Accertarsi che la connessione di rete tra l'appliance virtuale di XClarity Administrator e il dispositivo sia attiva. Se si trovano in segmenti di rete diversi, accertarsi che tra i due segmenti sia operativa l'instradabilità della rete.
- Una o più impostazioni di configurazione nel pattern server determinano una modifica delle impostazioni non valida nel dispositivo gestito selezionato. Tenere in considerazione i seguenti esempi.
  - Il pattern UEFI estesa selezionato non è compatibile con il dispositivo selezionato.

    Ad esempio, se un pattern UEFI fornito con XClarity Administrator per un server basato su X6 (ad esempio, System x3950 X6) è selezionato e distribuito in un server System x3650 M4, le differenze nelle impostazioni del processore tra i due server potrebbero impedire l'attivazione del profilo. Per risolvere il problema, accertarsi che il pattern UEFI estesa selezionato sia compatibile con il server selezionato.
  - Un pattern porta per una porta dell'adattatore Ethernet viene assegnato a una porta che non supporta le impostazioni selezionate.

    Ad esempio, negli adattatori basati su Emulex, alcune impostazioni sono esposte solo sulla prima porta dell'adattatore, nello specifico le impostazioni di modalità avanzata e porta utilizzate per disabilitare una porta. Se queste impostazioni vengono assegnate alla seconda porta dell'adattatore, potrebbe verificarsi un errore di attivazione. Questi problemi potrebbero essere rappresentati nei messaggi del processo come `AdvancedMode non è un'impostazione` o `Port1 non è un'impostazione`. Per risolvere il problema, accertarsi che il pattern porta che include queste impostazioni Pattern porta estesi per la modalità avanzata o l'abilitazione della porta sia assegnato solo alla prima porta dell'adattatore.

© Copyright Lenovo 2015, 2025

– Dopo un aggiornamento firmware, alcune impostazioni non sono supportate sul dispositivo gestito selezionato.

  Ad esempio, dopo l'aggiornamento del firmware di un adattatore I/O, alcune impostazioni potrebbero essere state rimosse o rinominate dal nuovo firmware e pertanto l'impostazione nel pattern server non è valida sul server di destinazione. Questi problemi sono rappresentati nel messaggio del processo come "xxx non è un'impostazione". Per risolvere il problema, è possibile importare un nuovo pattern server dal server, in modo che il nuovo pattern includa tutte le impostazioni supportate dal nuovo firmware. Se è necessario continuare a utilizzare il vecchio pattern, modificare manualmente il pattern server per rimuovere le impostazioni non valide.

- Si verifica un errore durante l'accensione o il riavvio del server quando è selezionata l'attivazione completa per la distribuzione del pattern o del profilo

  Accertarsi che lo stato di alimentazione del dispositivo sia indicato correttamente in XClarity Administrator. In caso contrario, aggiornare l'inventario per sincronizzare lo stato di alimentazione:

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).
  2. Selezionare il server e fare clic su **Tutte le azioni → Aggiorna inventario**.

Configurazione non valida distribuita in uno switch

Utilizzare queste informazioni per risolvere i problemi di distribuzione di una configurazione non valida in uno switch

È necessario creare ID VLAN prima di aggiungere una porta a una specifica rete VLAN. Se un pattern porta contiene impostazioni VLAN di porta interna dello switch con ID VLAN non preconfigurati per lo switch, l'attivazione del profilo potrebbe avere esito positivo, ma sarà necessario correggere la configurazione non applicata e non valida sullo switch.

Per risolvere il problema, eseguire il login allo switch e configurare manualmente i prerequisiti oppure rifiutare le modifiche distribuendo un pattern con impostazioni valide.

Capitolo 15. Problemi del repository e dell'aggiornamento firmware

Utilizzare queste informazioni per risolvere problemi relativi all'aggiornamento firmware.

Impossibile connettersi al repository Lenovo

Lenovo XClarity Administrator v 2.8 e le versioni precedenti utilizzano una connessione HTTP al supporto Lenovo per aggiornare il catalogo degli aggiornamenti firmware e per scaricare i pacchetti di aggiornamento; tuttavia, il supporto Lenovo richiede ora una connessione HTTPS.

Installare la versione più recente di GAFix sull'istanza di XClarity Administrator oppure eseguire l'aggiornamento a XClarity Administrator v 3.0.0 o successiva.

Dopo l'aggiornamento firmware, Applica/Attiva non mostra la versione firmware aggiornata

Utilizzare queste informazioni per risolvere i problemi relativi alla pagina Aggiornamenti firmware: Applica/Attiva.

Verificare che venga confrontato l'inventario più recente facendo clic sull'icona **Aggiorna** ( ) nella pagina Aggiornamenti firmware: Applica/Attiva per richiedere una sincronizzazione con i dati dell'appliance Lenovo XClarity Administrator.

Impossibile aggiornare il firmware di un dispositivo

Utilizzare queste informazioni per risolvere i problemi di aggiornamento del firmware nei dispositivi gestiti.

- Consultare Considerazioni sull'aggiornamento del firmware nella documentazione online di XClarity Administrator e seguire i suggerimenti forniti.
- Assicurarsi che lo stato del server non sia offline e che sia raggiungibile in rete da Lenovo XClarity Administrator.
- Se si verifica un problema durante l'aggiornamento del firmware su uno switch FC5022 con FOS v7.4.x e versioni precedenti, eseguire il seguente comando da un'interfaccia della riga di comando. Per ulteriori informazioni, vedere Suggerimento tecnico HT507915.
  ```
  Seccrypto -- default -type SSH -force
  ```

Blocco dell'aggiornamento firmware di CMM

Utilizzare queste informazioni per risolvere i problemi di aggiornamento del firmware CMM, stack Flex versione 1.3.2.1 da 2PET12K a 2PET12Q, che è in esecuzione da più di tre settimane e fa parte di una configurazione con due moduli CMM.

1. Eseguire un riposizionamento virtuale del modulo CMM. In presenza di due moduli CMM nello stesso chassis, riposizionare virtualmente i due moduli CMM contemporaneamente. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.
2. Eseguire nuovamente l'aggiornamento da XClarity Administrator.

© Copyright Lenovo 2015, 2025

Il firmware viene aggiornato ma non viene eseguito il controllo di conformità

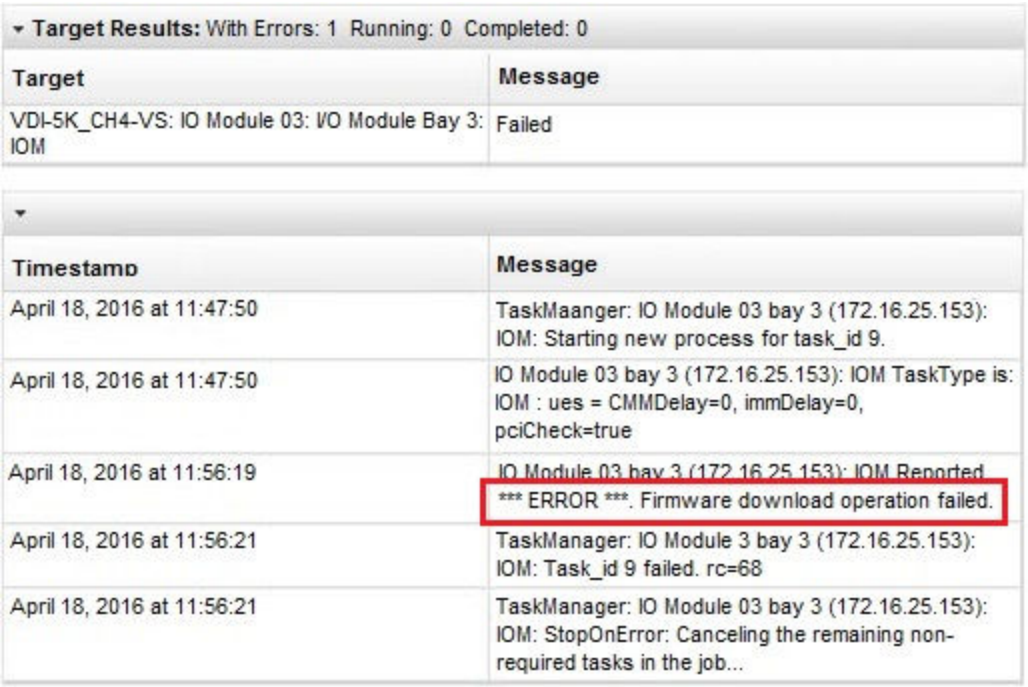
Utilizzare queste informazioni per risolvere problemi di conformità in seguito a un aggiornamento firmware.

Eseguire un riposizionamento virtuale sul dispositivo oppure eseguire un ulteriore aggiornamento, ad esempio dell'unita disco fisso.

Aggiornamenti firmware degli switch Flex System non riusciti

I seguenti argomenti descrivono gli errori che possono essere indicati nel log dei processi.

Per individuare i messaggi, fare clic su **Monitoraggio → Processi** dal menu di Lenovo XClarity Administrator. Il messaggio di errore può essere individuato facendo clic sul collegamento per il processo nella colonna **Processi** per visualizzare la finestra di dialogo di riepilogo e dei risultati. Sotto la sezione Risultati destinazione, il messaggio è elencato nella colonna **Messaggio** e inizia con "***ERRORE***".



Target Results: With Errors: 1 Running: 0 Completed: 0

Target	Message
VDI-5K_CH4-VS: IO Module 03: I/O Module Bay 3: IOM	Failed

Timestamp	Message
April 18, 2016 at 11:47:50	TaskMaanger: IO Module 03 bay 3 (172.16.25.153): IOM: Starting new process for task_id 9.
April 18, 2016 at 11:47:50	IO Module 03 bay 3 (172.16.25.153): IOM TaskType is: IOM : ues = CMMDelay=0, immDelay=0, pciCheck=true
April 18, 2016 at 11:56:19	IO Module 03 bay 3 (172.16.25.153): IOM Reported *** ERROR ***. Firmware download operation failed.
April 18, 2016 at 11:56:21	TaskManager: IO Module 3 bay 3 (172.16.25.153): IOM: Task_id 9 failed. rc=68
April 18, 2016 at 11:56:21	TaskManager: IO Module 03 bay 3 (172.16.25.153): IOM: StopOnError: Canceling the remaining non-required tasks in the job...

Importante: Talvolta potrebbero verificarsi degli errori durante gli aggiornamenti firmware degli switch Flex con XClarity Administrator. In presenza di errori, seguire i suggerimenti nei seguenti argomenti. Se gli aggiornamenti firmware dello switch Flex con XClarity Administrator continuano a causare errori, aggiornare gli switch Flex direttamente dall'interfaccia dello switch Flex.

Nota: Gli aggiornamenti firmware a uno switch Flex System potrebbero non riuscire se lo switch non esegue EHCM L3. Per ulteriori informazioni, vedere Considerazioni sull'aggiornamento del firmware nella documentazione online di XClarity Administrator.

Aggiornamento firmware sullo switch Flex System non riuscito con messaggio di errore "Operazione di download del firmware non riuscita".

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato Operazione di download del firmware non riuscita` nel log dei processi. Ciò potrebbe verificarsi sugli switch EN4023 e

FC5022 se si tenta di eseguire un aggiornamento invasivo che richiede di ignorare una versione dell'aggiornamento firmware precedente e passare direttamente alla più recente.

Per risolvere questo problema, aggiornare lo switch Flex direttamente dalla relativa CLI o dall'interfaccia Web.

Per FC5022, la migrazione da FOS v7.3 a v8.0.1-pha costituisce un aggiornamento con interruzioni. La migrazione da FOS v7.4 a FOS v8.0.1-pha costituisce un aggiornamento senza interruzioni.

È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore "DCSS_RC_CDT_FAIL"

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato DCSS_RC_CDT_FAIL` nel log dei processi. Indica che lo switch Flex potrebbe essere spento o potrebbero essersi verificati altri problemi di comunicazione.

Eseguire le seguenti azioni in questo ordine. Dopo ogni passaggio, tentare di nuovo l'aggiornamento del firmware.

1. Verificare che lo switch Flex sia acceso.
2. Verificare che lo switch Flex abbia un indirizzo IP valido.
3. Reimpostare lo switch Flex.
4. Reimpostare/riavviare CMM.

Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di "timeout"

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato Timeout` nel log dei processi. Ciò potrebbe verificarsi se Lenovo XClarity Administrator non è in grado di raggiungere in rete l'indirizzo IP dello switch.

Eseguire le seguenti azioni in questo ordine. Dopo ogni passaggio, tentare di nuovo l'aggiornamento del firmware.

1. Verificare che lo switch Flex abbia un indirizzo IP valido e che sia raggiungibile in rete da XClarity Administrator.
2. Reimpostare lo switch Flex.
3. Reimpostare/riavviare CMM.

Aggiornamento firmware per lo switch Flex non riuscito, con il messaggio di errore "Impossibile scaricare la stessa versione firmware. Scaricare un altro firmware."

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato Impossibile scaricare la stessa versione firmware. Scaricare un altro firmware.` nel log dei processi. Questa condizione potrebbe verificarsi se si tenta di aggiornare lo switch EN4023 allo stesso livello.

Lo switch EN4023 non consente di aggiornare il firmware allo stesso livello già in esecuzione.

Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di contatto host non riuscito

Utilizzare queste informazioni per risolvere un messaggio di errore IOM: ***ERROR*** segnalato Contatto host non riuscito nel log dei processi. Ciò potrebbe verificarsi se Lenovo XClarity Administrator non è in grado di raggiungere in rete l'indirizzo IP dello switch.

Eseguire le seguenti azioni in questo ordine. Dopo ogni passaggio, tentare di nuovo l'aggiornamento del firmware.

1. Verificare che lo switch abbia un indirizzo IP valido e che sia raggiungibile in rete da XClarity Administrator.
2. Riavviare lo switch.
3. Riavviare il modulo CMM.

Aggiornamento firmware dello switch Flex non riuscito con messaggio di errore di "file inesistente"

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato File inesistente` nel log dei processi. Ciò potrebbe verificarsi se Lenovo XClarity Administrator non è in grado di raggiungere in rete l'indirizzo IP dello switch.

Eseguire le seguenti azioni in questo ordine. Dopo ogni passaggio, tentare di nuovo l'aggiornamento del firmware.

1. Verificare che lo switch abbia un indirizzo IP valido e che sia raggiungibile in rete da XClarity Administrator.
2. Reimpostare lo switch.
3. Reimpostare/riavviare CMM.

Aggiornamento firmware dello switch Flex non riuscito con messaggio di "flashing concluso con errore"

Utilizzare queste informazioni per risolvere un messaggio di errore `IOM: ***ERROR*** segnalato Flashing concluso con errore` nel log dei processi. Ciò potrebbe verificarsi se lo switch non dispone di un indirizzo IP valido.

Verificare che lo switch abbia un indirizzo IP valido e che sia raggiungibile in rete da Lenovo XClarity Administrator.

Aggiornamento firmware dello switch Ethernet EN6131 40 Gb o dello switch InfiniBand IB6131 non riuscito

Utilizzare queste informazioni per correggere un errore imprevisto durante l'aggiornamento firmware di EN6131 40 Gb Ethernet Switch o IB6131 InfiniBand Switch.

1. Cercare nel log dei processi un messaggio di errore dello switch, ad esempio `Spazio su disco insufficiente per scaricare l'immagine`.

   Nota: Nel log dei processi potrebbero essere presenti ulteriori informazioni. Spesso, il messaggio è nel formato `IOM: ***ERROR*** segnalato` *msg*, dove *msg* è l'errore specifico per il modulo.
2. Verificare la velocità e la stabilità della rete. L'aggiornamento del firmware potrebbe non riuscire se non viene completato entro 30 minuti.
3. Liberare una quantità di spazio su disco nello switch sufficiente per il file di aggiornamento. Lo spazio su disco viene utilizzato durante la copia dei file di aggiornamento nello switch. Vedere la Switch Ethernet 40

Gb Lenovo Flex System EN6131 nella documentazione online di Flex Systems per le istruzioni sulla gestione dello spazio su disco.

4. Eseguire nuovamente l'aggiornamento da Lenovo XClarity Administrator.

Aggiornamento firmware di Lenovo EN4091 pass-thru module non riuscito

Utilizzare queste informazioni per correggere un errore imprevisto durante l'aggiornamento firmware del modulo pass-thru Lenovo EN4091.

1. Cercare nel log dei processi un messaggio di errore del modulo pass-thru, ad esempio `Immagine del firmware con errore relativo all'integrità dei dati` o `Contatto host non riuscito`.

   Nota: Nel log dei processi potrebbero essere presenti ulteriori informazioni. Spesso, il messaggio è nel formato `IOM: ***ERROR*** segnalato` *msg*, dove *msg* è l'errore specifico per il modulo.
2. Eseguire un riposizionamento virtuale del modulo Lenovo EN4091.
3. Eseguire nuovamente l'aggiornamento da Lenovo XClarity Administrator.

Aggiornamento firmware dello switch Flex System non riuscito con messaggio di errore "Autenticazione chiave host non riuscita"

Nel log dei processi viene visualizzato un messaggio di errore nel formato "IOM: ***ERROR*** segnalato Autenticazione chiave host non riuscita". Questa situazione si verifica quando la chiave SFTP è stata modificata in un server SFTP precedentemente utilizzato per aggiornare lo switch Flex System. Gli switch coinvolti sono CN4093, EN2092, EN4091, EN4093, EN4093R, SI4093.

In Lenovo XClarity Administrator questo errore può verificarsi se il firmware è stato già aggiornato su uno switch Flex System e successivamente si installa un'altra versione successiva di XClarity Administrator oppure si riavvia XClarity Administrator e successivamente si tenta di aggiornare lo switch. L'installazione di una nuova versione di XClarity Administrator o il riavvio di XClarity Administrator potrebbe infatti determinare la generazione di una nuova chiave SFTP.

Per risolvere il problema, immettere il seguente comando dalla CLI di uno switch Flex System o Lenovo Flex System per eliminare le chiavi SSH. Se lo switch utilizza lo standard ISCLI, è necessario accedere alla modalità del terminale di configurazione per eseguire il comando. Per passare alla modalità del terminale di configurazione, eseguire i comandi `enable` e `configure terminal`.

```
clear ssh-clienthostkey all
```

Nota: Se lo switch Flex System è in modalità IBMNOS CLI, immettere i seguenti comandi dalla CLI dello switch per eliminare le chiavi SSH:

```
maint
clssh
all
exit
```

Quando si esegue un aggiornamento, il sistema non riesce a entrare in modalità di manutenzione

Utilizzare queste informazioni per risolvere i problemi relativi agli aggiornamenti firmware e alla modalità di manutenzione.

Riprovare l'aggiornamento firmware.

Il riavvio di un server dal sistema operativo non attiva la modalità di manutenzione

Durante l'aggiornamento del firmware con attivazione ritardata in uno dei seguenti server, lo stato di aggiornamento mostra "Modalità manutenzione in sospeso" anche dopo aver riavviato il server dal sistema operativo.

- Flex System x240 M5, tipi 2591 e 9532
- NeXtScale nx360 M5, tipo 5465
- System x3250 M6, tipi 3633 e 3943
- System x3550 M5, tipo 5463
- System x3500 M5, tipo 5464
- System x3550 M5, Tipo 8869
- System x3650 M5, tipo 5462
- System x3650 M5, Tipo 8871

Per risolvere il problema, riavviare il server dall'interfaccia Web del controller di gestione. Una volta ripristinato il server, riprenderà il processo di aggiornamento dell'attivazione.

Il server che esegue Red Hat Enterprise Linux (RHEL) non si riavvia

Per Red Hat® Enterprise Linux (RHEL) v7 e versioni successive, riavviare il sistema operativo da una modalità grafica consente di sospendere il server per impostazione predefinita.

Configurare manualmente RHEL per modificare il comportamento del pulsante di alimentazione su Spegni. Per istruzioni, vedere Guida di amministrazione e migrazione dei dati di Red Hat: modifica del comportamento in caso di pressione del pulsante di alimentazione in modalità di destinazione grafica.

Capitolo 16. Problemi del repository e di aggiornamento dei driver di dispositivo del sistema operativo

Utilizzare queste informazioni per risolvere problemi relativi all'aggiornamento dei driver di dispositivo del sistema operativo.

Impossibile connettersi al sito Web del supporto Lenovo per scaricare gli aggiornamenti dei driver di dispositivo

Utilizzare queste informazioni per risolvere i problemi di download di UpdateXpress System Packs (UXSPs) e dei driver di dispositivo dal sito Web del supporto Lenovo.

- Accertarsi che la porta dell'appliance Lenovo XClarity Administrator (eth0 o eth1) configurata per la gestione disponga di accesso Internet. Per ulteriori informazioni sulle interfacce di rete, vedere Considerazioni sulla rete nella documentazione online di XClarity Administrator.
- Verificare che tutte le porte richieste e gli indirizzi Internet siano disponibili prima di tentare di aggiornare i driver di dispositivo su un server gestito. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta e Firewall e server proxy nella documentazione online di XClarity Administrator.

Non è possibile aggiornare i driver di dispositivo su un server

Utilizzare queste informazioni per risolvere i problemi di aggiornamento dei driver di dispositivo su un server gestito.

- Verificare che il server sia online e raggiungibile in rete da Lenovo XClarity Administrator.
- Esaminare le considerazioni sull'aggiornamento dei driver di dispositivo (vedere Considerazioni sull'aggiornamento dei driver di dispositivo del sistema operativo nella documentazione online di XClarity Administrator).

© Copyright Lenovo 2015, 2025

Capitolo 17. Problemi di distribuzione del sistema operativo

Utilizzare queste informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di distribuire sistemi operativi nei server gestiti da Lenovo XClarity Administrator.

Per problemi generici correlati alla distribuzione dei sistemi operativi, vedere Impossibile distribuire un sistema operativo.

Problemi di report dello stato durante la distribuzione del sistema operativo

Utilizzare queste informazioni per risolvere i problemi di report dello stato di Lenovo XClarity Administrator durante la distribuzione del sistema operativo.

- Durante la distribuzione di VMware 6.5 o versione successiva mediante XClarity Administrator v1.4.0 e versioni precedenti, lo stato del processo potrebbe segnalare che la distribuzione è stata completata prima che il sistema operativo sia pronto.

  Quando si utilizzano script per monitorare il completamento della distribuzione del sistema operativo, aggiungere un ritardo di 10 minuti allo script dopo la ricezione dello stato del processo di distribuzione che indica il completamento della distribuzione del sistema operativo.
- Durante la distribuzione di Windows su una rete che utilizza l'etichettatura VLAN, potrebbero essere segnalati errori di stato durante il *passaggio di configurazione specializzato* della distribuzione.

  È possibile ignorare questi errori.

Impossibile distribuire un sistema operativo

Utilizzare queste informazioni per risolvere problemi generici che si potrebbero riscontrare nel tentativo di distribuire un sistema operativi in un server gestito da Lenovo XClarity Administrator.

In ambienti di rete lenti, la distribuzione del sistema operativo di SLES 12 e 12.1 in modalità IP statico potrebbe avere esito negativo, poiché il parametro di avvio ritardato della rete non è effettivo in tale modalità. Questa problema è stato corretto in SLES 12.2.

Per risolvere il problema, procedere come segue:

1. Per i Server ThinkSystem V3 e V4 (con XCC2 o XCC3) con Protezione del sistema abilitato e l'azione impostata su **Impedisci avvio del sistema operativo**, verificare che Protezione del sistema sia conforme sul dispositivo. Se Protezione del sistema non è conforme, ai dispositivi viene impedito il completamento del processo di avvio, determinando un errore della distribuzione del sistema operativo. Per eseguire il provisioning di questi dispositivi, rispondere manualmente al prompt di avvio di Protezione del sistema per consentire l'avvio normale dei dispositivi.
2. Se viene visualizzato il messaggio `https://<management_server_IP>/osdeployment/connection/... Autorizzazione negata`, aggiornare il BIOS del server e impostare la data e l'ora correnti.
3. Controllare tutti i requisiti per il sistema operativo da distribuire. Vedere Sistemi operativi supportati nella documentazione online di XClarity Administrator.Ad esempio:
   - Potrebbe verificarsi un problema con la distribuzione di VMware ESXi se lo spazio I/O mappato dalla memoria (MMIO) non è stato impostato su almeno 3 GB.

© Copyright Lenovo 2015, 2025

- Se si distribuisce Microsoft Windows e si esegue l'aggiunta a un dominio Active Directory, seguire le considerazioni descritte in Integrazione con Windows Active Directory nella documentazione online di XClarity Administrator.

4. Esaminare le limitazioni di supporto relative alla distribuzione dei sistemi operativi per specifici adattatori I/O. Per informazioni sul supporto degli adattatori I/O, vedere la Supporto XClarity Administrator - Pagina Web sulla compatibilità.
5. Verificare la stabilità della connessione di rete tra XClarity Administrator e il dispositivo (server gestito) in cui verrà installato il sistema operativo.

   Nota: Nel caso di SLES 11 SP4, la distribuzione potrebbe arrestarsi e non riavviarsi se viene persa la connessione di rete tra XClarity Administrator e il dispositivo. In questo caso, controllare l'ambiente di rete e ridistribuire il sistema operativo.
6. Accertarsi che almeno una porta di rete in XClarity Administrator sia impostata per la gestione e la distribuzione delle immagini di sistemi operativi.È possibile configurare la topologia di rete di XClarity Administrator dalla pagina Accesso alla rete. Per ulteriori informazioni sulla pagina Accesso alla rete, vedere Configurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.
7. Accertarsi che la porta di rete di XClarity Administrator utilizzata per la connessione alla rete di dati sia configurata in modo da condividere la stessa rete delle porte di rete di dati sul server gestito. La porta del server viene specificata dall'indirizzo MAC ed è configurabile mediante la pagina Sistemi operativi - > Impostazioni di rete. Per ulteriori informazioni sulla modifica delle impostazioni di rete, vedere Configurazione delle impostazioni di rete per i server gestiti nella documentazione online di XClarity Administrator.
8. Verificare che il server di destinazione non abbia un pattern server rinviato o parziale attivato. Se un pattern server è stato rinviato o parzialmente attivato sul server di destinazione, riavviare il server per applicare tutte le impostazioni di configurazione.
9. Visualizzare lo stato del server dalla pagina Distribuisci immagini sistema operativo per accertarsi che sia impostato su "Pronto". Se lo stato è "Non pronto", fare clic sul collegamento dello stato per determinare il motivo per cui il server non è pronto per la distribuzione dei sistemi operativi.Per ulteriori informazioni sulla distribuzione di sistemi operativi, vedere Distribuzione di un'immagine del sistema operativo nella documentazione online di XClarity Administrator.
10. Accertarsi che il dispositivo disponga di visibilità sulla posizione di storage selezionata per la distribuzione di sistemi operativi.

    Suggerimento: per verificare che le distribuzioni dei sistemi operativi vengano completate correttamente, rimuovere tutto lo storage dal server, ad eccezione dello storage scelto per la distribuzione dei sistemi operativi.

Impossibile importare un file nel repository di immagini del sistema operativo

Utilizzare questa sezione di informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di importare file nel repository di immagini di Lenovo XClarity Administrator.

Per risolvere il problema, procedere come segue:

- Accertarsi che il file in fase di importazione sia stato verificato con il test checksum.
- Accertarsi che il sistema operativo di base sia supportato da XClarity Administrator. Vedere Sistemi operativi supportati nella documentazione online di XClarity Administrator.
- Se si sta eseguendo un'importazione dal sistema locale:
  - I browser Internet Explorer e Microsoft Edge hanno un limite di caricamento di 4 GB. Se il file da importare è maggiore di 4 GB, considerare la possibilità di utilizzare un altro browser Web (come Chrome o Firefox)

- Se si sta eseguendo un'importazione da un file server remoto:
  - Verificare che il percorso completo al file corrisponda al percorso effettivo sul file server remoto.
  - Verificare che il percorso completo al file contenga le barre o le barre rovesciate corrette, a seconda del sistema operativo che ospita il file server remoto.
  - Verificare che la directory sul file server remoto disponga delle autorizzazioni necessarie.
  - Verificare che vi sia spazio sufficiente sul disco del repository di immagini del sistema operativo per memorizzare il file (vedere Gestione dello spazio su disco nella documentazione online di XClarity Administrator).
  - Accertarsi di avere eseguito il login al file server remoto utilizzando le credenziali corrette.
  - Verificare che sia disponibile una connessione di rete stabile tra XClarity Administrator e il file server remoto.
  - Verificare che siano stati importati i certificati attendibili corretti e che i certificati non siano stati revocati (vedere Utilizzo dei certificati di sicurezza nella documentazione online di XClarity Administrator).
  - Verificare che il file server remoto supporti almeno un algoritmo supportato da XClarity Administrator per ogni tipo di algoritmo richiesto da SSH (vedere Implementazione di un ambiente sicuro nella documentazione online di XClarity Administrator).

Il programma di installazione del sistema operativo non è in grado di trovare l'unità disco su cui si desidera eseguire l'installazione

Per i server che includono adattatori RAID software (come 110i AnyRAID, ServeRAID C100 o C105 e Intel RSTe SATA Software RAID), se l'adattatore SATA è abilitato nel controller di gestione, la modalità SATA deve essere impostata su "AHCI". Altre modalità (come "RAID" e "IDE") non sono supportate per il software RAID dai sistemi operativi RHEL, SUSE, VMware o Windows.

Nota: Ciascun server deve essere dotato di un adattatore RAID hardware installato e configurato. Il RAID software generalmente presente sull'adattatore di storage Intel SATA integrato non è supportato. Tuttavia, se non è presente un adattatore RAID hardware, impostando l'adattatore SATA in modalità SATA AHCI, in alcuni casi la distribuzione del sistema operativo potrebbe andare a buon fine.

Per modificare la modalità SATA per ThinkServer, completare le seguenti operazioni.
1. Da AMI Setup Utility selezionare il menu **Advanced Settings**.
2. Utilizzare i tasti freccia per selezionare **SATA Mode**.
3. Premere **+** per modificare il valore in `AHCI`.
4. Premere **F10** per salvare la modifica.

Per modificare la modalità SATA per altri server, completare le seguenti operazioni.
1. Da F1 Setup Utility, selezionare il menu **System Settings → Devices and I/O Ports → Onboard SATA Mode**.
2. Premere **+** per modificare il valore in `AHCI`.
3. Premere **F10** per salvare la modifica.

Impossibile avviare il programma di installazione del sistema operativo su un server ThinkServer

Per i server ThinkServer, il criterio OpROM di storage in ThinkServer Management Module devono essere impostati su "UEFI Only" per consentire l'avvio dell'immagine del programma di installazione del sistema operativo. Se il criterio è impostato su "Legacy Only," il programma di installazione del sistema operativo non verrà avviato.

Per modificare il criterio OpROM di storage, attenersi alla procedura descritta di seguito.

1. Da AMI Setup Utility selezionare il menu **Boot Manager → Miscellaneous Boot Settings**.
2. Utilizzare i tasti freccia per selezionare **Storage OpROM Policy**.
3. Premere **+** per modificare il valore in `UEFI Only`.
4. Premere **F10** per salvare la modifica.

Per ulteriori informazioni, consultare la documentazione di ThinkServer.

Problemi di distribuzione di VMware ESXi

Utilizzare queste informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di distribuire i sistemi operativi VMware ESXi nei server gestiti da Lenovo XClarity Administrator.

Blocco o riavvio del sistema causato dalla distribuzione VMware

Durante l'installazione di VMware 5.1u1, 5.1u2, 5.1u3 o 5.5 (qualsiasi aggiornamento) in un server gestito, il server potrebbe bloccarsi o riavviarsi.

Il blocco o il riavvio potrebbe verificarsi subito dopo aver visualizzato il seguente messaggio:
```
Loading image.pld
```

VMware 5.5 richiede la configurazione dello spazio I/O mappato dalla memoria (MMIO) nei 4 GB iniziali del server. A seconda della configurazione, alcuni server tentano di utilizzare più di 4 GB di memoria. Ciò potrebbe causare un errore.

Per risolvere il problema, procedere come segue:

Suggerimento: anziché impostare **MM Config** tramite Setup Utility per ciascun server, valutare la possibilità di utilizzare uno dei pattern UEFI estesa predefiniti relativi alla virtualizzazione, che imposta l'opzione MM Config su 3 GB e disabilita l'assegnazione di risorse PCI a 64 bit. Per ulteriori informazioni su questi pattern, vedere Definizione delle impostazioni UEFI estese nella documentazione online di XClarity Administrator.

1. Riavviare il sistema. Quando viene visualizzato `Press <F1> Setup`, premere F1.
2. Selezionare **System Settings → Devices and I/O ports**.
3. Modificare l'impostazione per **MM Config** da 2 GB a 3 GB.
4. Accertarsi che l'impostazione per **PCI 64-Bit Resource** sia impostata su Disable.
5. Tentare di installare di nuovo l'immagine VMware.

Distribuzione VMware non riuscita con errori del disco

Durante l'installazione di VMware ESXi, potrebbe essere visualizzato un errore relativo all'unità disco e la distribuzione ha esito negativo.

Il messaggio di errore potrebbe essere simile al seguente esempio:
```
error:/tmp/partitioning:line 2: install requires --disk
or --firstdisk
error:/tmp/partitioning:line 1: clearpart requires
one of the following arguments: --alldrives, --firstdisk,
--ignoredrives=, --drives=
```

Questo errore potrebbe verificarsi se il programma di installazione di ESXi non rileva una configurazione SAS disponibile per la formattazione e l'installazione. In genere, significa che la configurazione RAID nel server è inattiva o configurata in modo errato. In alternativa, questo errore potrebbe verificarsi se un pattern server è stato distribuito tramite Lenovo XClarity Administrator ed è stata selezionata l'opzione **Disabilita disco locale** per il pattern.

Per risolvere il problema, procedere come segue:

- Se un pattern server è stato distribuito in questo server ed è stata selezionata l'opzione **Disabilita disco locale**, aggiornare il pattern server e ridistribuirlo. Per ulteriori informazioni sulla configurazione dello storage locale mediante pattern server, vedere Definizione di storage locale nella documentazione online di XClarity Administrator.
- Confermare che la configurazione RAID è corretta sul server:
  1. Riavviare il server e tentare l'avvio in un'opzione legacy premendo F12 (scegliere un'opzione come HD0).
  2. Durante l'avvio, quando verranno visualizzate le informazioni sull'adattatore LSI SAS, premere CTRL +C per modificare la configurazione.
  3. Una volta visualizzata l'interfaccia utente, selezionare **Proprietà RAID** e **Visualizza configurazione esistente**.
     - Se **Visualizza configurazione esistente** non è visibile, il RAID non è stato configurato.
     - Se la configurazione esistente mostra lo stato "Inattivo," assicurarsi che il RAID sia configurato correttamente.

Il sistema operativo non si riavvia per completare la distribuzione di ESXi su un server ThinkServer

Utilizzare queste informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di distribuire i sistemi operativi VMware ESXi sui server gestiti da Lenovo XClarity Administrator, con l'opzione PXE abilitata su una scheda di rete o su periferiche avviabili diverse dall'unità di installazione inclusa nell'elenco dell'ordine di avvio.

Quando si distribuisce ESXi su un server ThinkServer, il sistema operativo non sposta in modo esplicito l'unità su cui è installato il sistema operativo alla prima voce dell'elenco dell'ordine di avvio. Se un dispositivo di avvio che contiene un server PXE o un sistema operativo avviabile viene specificato prima del dispositivo di avvio che contiene ESXi, ESXi non si avvia. Per la distribuzione di ESXi, XClarity Administrator aggiorna l'elenco dell'ordine di avvio per la maggior parte dei server, al fine di verificare che il dispositivo di avvio ESXi sia il primo nell'elenco dell'ordine di avvio; tuttavia, i server ThinkServer non dispongono di una funzionalità che consenta a XClarity Administrator di aggiornare l'elenco dell'ordine di avvio.

Se il server ThinkServer dispone di schede di rete con avvio PXE, disabilitare il supporto PXE sulle schede di rete, ridistribuire il sistema operativo e quindi riabilitare il supporto PXE. Premere F12 per intercettare l'avvio e visualizzare le impostazioni PXE. Per informazioni sulla modifica delle impostazioni di avvio PXE, consultare la documentazione della scheda di rete.

Se nell'elenco dell'ordine di avvio del server ThinkServer sono presenti periferiche avviabili diverse dall'unità su cui deve essere installato il sistema operativo, rimuovere le periferiche avviabili dall'elenco dell'ordine, ridistribuire il sistema operativo e quindi aggiungere nuovamente la periferica avviabile all'elenco. Verificare che l'unità installata sia la prima dell'elenco. Per informazioni sulla modifica dell'elenco dell'ordine di avvio, consultare la documentazione di ThinkServer.

Problemi di distribuzione dei sistemi operativi Linux Red Hat e SUSE

Utilizzare queste informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di distribuire i sistemi operativi Red Hat e SUSE Linux sui server gestiti da Lenovo XClarity Administrator.

Distribuzione di Red Hat 6.x non riuscita su server basati su rack con IP statico

Potrebbe verificarsi un problema nel caso in cui si tenti di distribuire Red Hat 6.x in un server gestito se tale server è collegato a uno switch TOR (Top-of-Rack). Se nello switch TOR l'opzione **spanning tree protocol** è abilitata e l'opzione **forward by default** è disabilitata, potrebbe non essere possibile scaricare l'immagine Red Hat nel server.

Per risolvere il problema, procedere come segue:

- Accertarsi che il server sia configurato per l'utilizzo del protocollo DHCP (e non di un indirizzo IP statico). Provare quindi a distribuire di nuovo il sistema operativo.
- Modificare la configurazione nello switch TOR per disabilitare l'opzione spanning tree protocol *oppure* abilitare l'opzione forward by default.

Distribuzione del sistema operativo non riuscita a causa di driver mancanti

Quando si distribuisce Red Hat® Enterprise Linux (RHEL) Server o SUSE® Linux Enterprise Server (SLES) su un server, è possibile che venga visualizzato un messaggio di errore che interrompe la distribuzione, causando il timeout del processo di distribuzione.

Questo errore potrebbe verificarsi se l'immagine del sistema operativo non contiene i driver per supportare tutti gli adattatori installati nel server gestito.

I driver esterni non vengono precaricati in Lenovo XClarity Administrator per determinati adattatori Mellanox IB. La distribuzione di RHEL o SLES su un server con questi adattatori Mellanox non è pertanto supportata. Per ulteriori informazioni sulle limitazioni degli adattatori Mellanox, vedere Pagina Web del supporto di Lenovo XClarity Administrator per gli adattatori Mellanox.

Problemi di distribuzione di Microsoft Windows

Utilizzare queste informazioni per risolvere i problemi che si potrebbero riscontrare nel tentativo di distribuire Microsoft Windows nei server gestiti da Lenovo XClarity Administrator.

La distribuzione del sistema operativo non riesce a causa di partizioni di sistema esistenti su un'unità disco collegata

Quando si distribuisce Microsoft Windows su un server, le unità disco collegate non devono disporre di partizioni di sistema esistenti. Se viene rilevata una partizione, la distribuzione del sistema operativo non riesce.

Per risolvere questo problema, completare una delle seguenti operazioni.

- Scollegare l'unità disco.
- Eliminare manualmente la partizione di sistema sull'unità disco collegata.

  Attenzione: L'eliminazione delle partizioni su un'unità disco potrebbe causare la perdita dei dati. Accertarsi di avere eseguito il backup di tutti i dati sull'unità disco prima di eliminare le partizioni.

  1. Da un prompt dei comandi di Windows, eseguire l'utilità `diskpart` (vedere Sito Web dei comandi DiskPart).
  2. Selezionare il disco digitando `select disk` <*number*>, dove <*number*> è il numero del disco che contiene la partizione che si desidera eliminare (vedere Sito Web per la selezione del disco).
  3. Selezionare la partizione da eliminare digitando `select partition` <*number*>, dove <*number*> è il numero della partizione sul disco selezionato (vedere Sito Web per la selezione della partizione).

4. Eliminare la partizione digitando `delete partition override`. I numeri della partizione e del disco sono inclusi nel log processi e nel messaggio di errore di WinPE che viene visualizzato al rilevamento di una partizione di sistema. (vedere Sito Web per l'eliminazione della partizione

Capitolo 18. Problemi di controllo remoto

Utilizzare queste informazioni per risolvere i problemi che potrebbero verificarsi quando si utilizza l'applicazione di controllo remoto in Lenovo XClarity Administrator.

La sessione di controllo remoto non si avvia

Utilizzare queste informazioni quando si tenta di avviare la sessione di controllo remoto dall'interfaccia Web di Lenovo XClarity Administrator o dal collegamento sul sistema, ma la sessione non viene avviata.

Per risolvere il problema, completare le seguenti operazioni.

1. Assicurarsi che il server a cui si sta effettuando il collegamento sia gestito da XClarity Administrator e che lo stato sia "Online" o "Normale". Per ulteriori informazioni sullo stato dei server, vedere Visualizzazione dello stato di un server gestito nella documentazione online di XClarity Administrator.
2. Verificare che le finestre di dialogo a comparsa non siano disabilitate nella sessione del browser Web.
3. Verificare che il browser Web abbia accettato i certificati di sicurezza da XClarity Administrator. Generalmente, viene richiesto di accettare il certificato al primo accesso a XClarity Administrator dal browser.
4. Dalla finestra "Controllo remoto", fare clic su **Preferenze → Generale → Sincronizza con il server di gestione** e attendere un minuto. Quindi, eseguire nuovamente la sessione di controllo remoto.
5. Per avviare l'applicazione, accertarsi di utilizzare una versione supportata di JRE.
   - In Internet Explorer, fare clic su **Strumenti → Opzioni Internet → Avanzate**. Assicurarsi che sia stata selezionata la versione corretta di JRE (JRE versione 7.0, aggiornamento 18 o successivo).
   - In Firefox, fare clic su **Strumenti → Opzioni → Applicazioni**. Verificare che Java Web Start Launcher sia associato al tipo di contenuto JNLP.

   Nota: Verificare che l'opzione **Usa formato ClientHello compatibile con SSL 2.0** *non sia* selezionata nel pannello di controllo Java.

   Se l'applicazione viene avviata dal collegamento sul desktop, assicurarsi che il sistema locale sia collegato a XClarity Administrator. L'applicazione convalida l'ID utente con il server di autenticazione XClarity Administrator.
6. Cancellare la cache Java Web Start sul sistema locale. Per cancellare la cache Java Web Start di un sistema su cui viene eseguito un sistema operativo Windows, eseguire il comando `javaws -uninstall`. Questa operazione può essere effettuata anche dal menu JAVA nel pannello di controllo di Windows.
7. Il controllo remoto richiede l'installazione di una chiave Features on Demand per ThinkServer System Manager Premium Upgrade sui server ThinkServer. Per ulteriori informazioni sulle chiavi FoD installate sui server, vedere Visualizzazione delle chiavi FoD (Feature on Demand) nella documentazione online diXClarity Administrator.

La sessione di controllo remoto si blocca dopo il login

Utilizzare queste informazioni per risolvere il problema di blocco della sessione di controllo remoto, dopo il login.

Se non si utilizza una versione supportata di JRE, la sessione di controllo remoto potrebbe bloccarsi dopo il login. Se la sessione di controllo remoto sembra bloccarsi dopo il login, per avviare l'applicazione, accertarsi di utilizzare una versione supportata di JRE:

- Oracle JRE versione 6.18 o successiva

© Copyright Lenovo 2015, 2025

Non è possibile connettersi a un server

Utilizzare queste informazioni per risolvere i problemi di avvio di una sessione di controllo remoto con un server.

Per risolvere questo problema, completare le seguenti operazioni.

- Assicurarsi di disporre dei privilegi **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** o **lxc-hw-manager**.
- Verificare che il sistema locale disponga della connettività di rete e che sia possibile collegarsi a Lenovo XClarity Administrator.
- Accertarsi che il server sia gestito da XClarity Administrator facendo clic su **Hardware → Server** dalla barra dei menu di XClarity Administrator.
- Se sul sistema locale è installato un firewall, verificare che siano consentite le connessioni all'indirizzo IP del server gestito.
- Eseguire il ping dell'indirizzo IP del server gestito per verificare che il sistema locale sia connesso al server gestito. Se si sta tentando di accedere a un server gestito da un sistema locale con un indirizzo IP di una rete esterna, anche il server gestito deve disporre di un indirizzo IP a cui sia possibile accedere esternamente.
- Verificare che il tunneling di XClarity Administrator non sia stato disabilitato, in modo che XClarity Administrator possa eseguire il tunneling delle richieste di controllo remoto al server gestito, indirizzabile in rete solo sulla rete di gestione privata. Il tunneling è abilitato per impostazione predefinita.È possibile abilitare il tunneling di XClarity Administrator dalla finestra di dialogo Preferenze del supporto remoto, nella scheda **Sicurezza**. Per ulteriori informazioni, vedere Impostazione delle preferenze di controllo remoto.

Impossibile comunicare con uno switch Flex System dopo l'avvio di una sessione di controllo remoto

Utilizzare queste informazioni per risolvere il problema quando Lenovo XClarity Administrator smette di comunicare con uno switch di rete Cisco Nexus B22 Fabric Extender dopo l'avvio di una sessione di controllo remoto.

Se il modulo CMM viene configurato per l'utilizzo del rilevamento automatico, verificare che la porta di rete sullo switch di rete Cisco Nexus B22 Fabric Extender sia configurata per utilizzare la modalità di negoziazione automatica.

Non è possibile connettersi a un server in modalità utente singolo

Utilizzare queste informazioni per risolvere i problemi di connessione a un server in modalità utente singolo.

Quando ci si collega a un server in modalità utente singolo, è possibile stabilire una sola sessione di controllo remoto al server alla volta.

Per risolvere il problema, completare i seguenti passaggi.

1. Tentare di collegarsi al server gestito in modalità multiutente (se consentito, in base ai requisiti di sicurezza).
2. Contattare altri utenti per determinare se è già stata stabilita una sessione di controllo remoto con il server gestito. In questo caso, attendere finché la sessione di controllo remoto con il server gestito non è terminata.
3. Tentare di collegarsi nuovamente al server gestito in modalità utente singolo.

Il controllo remoto si connette a un server, ma non è disponibile alcun video

Utilizzare queste informazioni per risolvere un problema di connessione a un server da una sessione di controllo remoto: durante la sessione viene visualizzato il messaggio `No video available`.

Assicurarsi che il server sia acceso e che la risoluzione e la velocità di aggiornamento utilizzate siano supportate dal sistema operativo.

Nella seguente tabella sono riportate le risoluzioni e le velocità di aggiornamento supportate.

Tabella 1. Risoluzioni e velocità di aggiornamento supportate

Risoluzione	**Velocità di aggiornamento**
640 x 480	60, 72, 75 e 85 Hz
800 x 600	60, 72, 75 e 85 Hz
1.024 x 768	60, 72, 75 e 85 Hz
1.440 x 900	60 Hz
1.280 x 1.024	60 e 75 Hz
1.680 x 1.050	60 Hz
1.600 x 1.200	60 e 75 Hz

Un server non viene visualizzato nell'elenco di aggiunta di una nuova sessione

Utilizzare queste informazioni per risolvere un problema di mancata visualizzazione di un server nell'elenco di aggiunta di una nuova sessione o se un server non viene più visualizzato nell'area miniature.

Per risolvere il problema, completare le seguenti operazioni.

1. Accertarsi che il server gestito sia gestito da Lenovo XClarity Administrator facendo clic su **Hardware → Server** dalla barra dei menu di XClarity Administrator.
2. Sincronizzare l'inventario facendo clic sulla scheda **Generale** dal menu di controllo remoto "Preferenza" e quindi su **Sincronizza con il server di gestione**. Per ulteriori informazioni sulle preferenze di controllo remoto, vedere Impostazione delle preferenze di controllo remoto nella documentazione online di XClarity Administrator.

Lo stato del server nella sessione di controllo remoto non corrisponde allo stato in Lenovo XClarity Administrator

Utilizzare queste informazioni per risolvere i problemi di mancata corrispondenza tra lo stato di un server gestito in una sessione di controllo remoto e lo stato del server gestito in Lenovo XClarity Administrator.

Per risolvere questo problema, completare le seguenti operazioni.

1. Accertarsi che il server sia gestito da XClarity Administrator facendo clic su **Hardware → Server** dalla barra dei menu di XClarity Administrator.
2. Sincronizzare l'inventario facendo clic sulla scheda **Generale** dal menu di controllo remoto "Preferenza" e quindi su **Sincronizza con il server di gestione**. Per ulteriori informazioni sulle preferenze di controllo remoto, vedere Impostazione delle preferenze di controllo remoto nella documentazione online di XClarity Administrator.

Un'unità o un'immagine non può essere montata su un server

Utilizzare queste informazioni per risolvere i problemi di montaggio di un'unità o un'immagine tramite supporti remoti, causati da unità o immagini che non è possibile montare.

Per risolvere il problema, completare le seguenti operazioni.

1. Interrompere e riavviare la sessione di controllo remoto.
2. Configurare la modalità di debug su "Completo" per la sessione di controllo remoto. È possibile configurare la modalità di debug da "Preferenze" nella pagina **Generale**. Quando si configura la modalità di debug su "Completo", la sessione di controllo remoto genera file di log di diagnostica. Per ulteriori informazioni sulla modalità di debug, Impostazione delle preferenze di controllo remoto.
3. Contattare Supporto Lenovo e fornire i file di log. Per ulteriori informazioni sull'invio dei dati diagnostici a Supporto Lenovo, vedere Utilizzo di assistenza e supporto.

L'opzione supporto di storage non viene visualizzata nell'elenco dei dispositivi di supporto remoto da montare

Utilizzare queste informazioni per risolvere i problemi relativi alla mancata visualizzazione dell'opzione supporto di storage nell'elenco dei dispositivi di supporto remoto disponibili per il montaggio.

Se un CD, un DVD o un dispositivo USB non viene visualizzato nell'elenco dei dispositivi di supporto remoto disponibili per il montaggio su un server gestito, fare clic su **Riavvia con account amministratore** dal pannello del supporto remoto per accedere a più dispositivi locali.

Non è possibile eseguire un'operazione relativa all'alimentazione

Utilizzare queste informazioni per risolvere i problemi di mancata esecuzione di un'operazione relativa all'alimentazione su un server gestito durante una sessione di controllo remoto.

Quando si tenta di eseguire un'operazione relativa all'alimentazione su un server gestito da una sessione di controllo remoto, è possibile che si riceva un messaggio di errore dell'operazione relativa all'alimentazione o di operazione non applicabile allo stato corrente del server gestito.

Per risolvere il problema, procedere come segue:

1. Assicurarsi che il server sia gestito da Lenovo XClarity Administrator. Per ulteriori informazioni, vedere Visualizzazione dello stato di un server gestito nella documentazione online di XClarity Administrator.
2. Dalla pagina "Server", verificare che lo stato del server sia valido.
3. Verificare che l'operazione relativa all'alimentazione sia valida per lo stato corrente del server. Ad esempio, se il server attualmente è spento, l'invio di un comando di spegnimento avrà esito negativo.
4. Controllare il log dei processi per verificare se l'operazione relativa all'alimentazione è stata completata. Il completamento dell'operazione potrebbe richiedere del tempo, a seconda del carico corrente di XClarity Administrator. Per ulteriori informazioni sulla visualizzazione dello stato dei processi, vedere Monitoraggio dei processi.

Il video non è disponibile quando si effettua il collegamento a Server Flex System x280 X6, x480 X6 e x880 X6

Utilizzare queste informazioni per risolvere i problemi di avvio di una sessione della console remota con un sistema multinodo Server Flex System x280 X6, x480 X6 e x880 X6 oppure quando nella nuova scheda non viene visualizzato alcun video.

Per risolvere il problema, completare le seguenti operazioni.

1. Se ancora attiva, termina la connessione appena avviata, chiudendo la nuova scheda.
2. Accertarsi di avviare una connessione remota con il server *primario* nella configurazione multinodo.

Capitolo 19. Problemi dell'interfaccia utente

Utilizzare queste informazioni per risolvere i problemi di interfaccia utente.

Le voci di menu, le icone delle barre degli strumenti e i pulsanti sono disabilitati (evidenziati in grigio)

Utilizzare queste informazioni per risolvere i problemi in caso di disabilitazione di determinate azioni nell'interfaccia utente.

Un *ruolo* viene utilizzato per controllare l'accesso utente alle risorse e limitare le azioni che gli utenti possono eseguire sulle risorse. Un *gruppo di ruoli* è una raccolta di uno o più ruoli che viene utilizzata per assegnare i ruoli a più utenti. I ruoli configurati per un gruppo di ruoli determinano il livello di accesso concesso a ciascun utente membro di questo gruppo di ruoli. Ogni utente Lenovo XClarity Administrator deve essere membro di almeno un gruppo di ruoli. Per informazioni sui ruoli e i privilegi, vedere Gestione dei ruoli nella documentazione online di XClarity Administrator.

Verificare che l'account utente sia assegnato a un gruppo di ruoli con i privilegi necessari per eseguire l'azione. Per ulteriori informazioni, contattare l'amministratore di sistema.

Il browser Web non risponde quando vengono aperte più schede

Quando vengono aperte più schede contenenti pagine di Lenovo XClarity Administrator, il browser Web potrebbe arrestarsi in modo anomalo o non rispondere

XClarity Administrator utilizza JavaScript lato client che si scambiano grandi quantità di dati con il server di gestione. Quando vengono aperte più schede, il browser Web utilizza più memoria, cicli di processore e larghezza di banda della rete. Diverse schede possano causare l'arresto anomalo o la mancata risposta di alcuni browser. L'effetto varia a seconda delle versioni e i tipi di browser Web.

Per risolvere questo problema, ridurre il numero di schede del browser Web che contengono pagine di XClarity Administrator.

Per ulteriori informazioni, vedere Suggerimento HT504133

Risposta JSON non riuscita con errore di analisi e altri errori imprevisti

Utilizzare queste informazioni per risolvere problemi relativi alla risposta JSON.

Provare ad effettuare il logout da Lenovo XClarity Administrator, per poi procedere a un nuovo login.

L'interfaccia utente non è visualizzata nella lingua preferita

Utilizzare queste informazioni per risolvere i problemi relativi alle preferenze della lingua.

1. Accertarsi che il browser Web utilizzi le impostazioni locali della lingua preferita.
2. Nella barra del titolo di Lenovo XClarity Administrator, fare clic sul menu azioni utente (

) e quindi su **Modifica lingua**. Selezionare la lingua che si desidera visualizzare, quindi fare clic su **Chiudi**.

© Copyright Lenovo 2015, 2025

Tempi di caricamento lenti o senza risposta, lunga attesa per l'aggiornamento, rendering inappropriato

Utilizzare queste informazioni per risolvere i problemi con l'interfaccia utente.

1. Aggiornare la pagina con il pulsante **Aggiorna** sul browser Web.
2. Cancellare la cache del browser Web e ricaricare la pagina.

Perdita di dati imprevista

Utilizzare queste informazioni per risolvere i problemi relativi alla perdita dei dati in Lenovo XClarity Administrator.

Se il sistema operativo host si è arrestato in modo imprevisto, ripristinare l'ultimo backup di XClarity Administrator (vedere Backup e ripristino di XClarity Administrator nella documentazione online di XClarity Administrator).

Le modifiche apportate alla posizione del dispositivo non vengono applicate nella vista rack

Utilizzare queste informazioni per risolvere i problemi della vista rack in Lenovo XClarity Administrator.

Se si modifica la posizione di un dispositivo utilizzando una delle seguenti API REST o il controller di gestione della scheda di base una volta gestito il dispositivo da parte di XClarity Administrator, le modifiche non verranno applicate nella vista rack nell'interfaccia utente di XClarity Administrator. Modificare le proprietà del dispositivo o il rack nell'interfaccia utente per applicare le modifiche apportate nell'API o nel controller di gestione (vedere Modifica delle proprietà di sistema per un server, Visualizzazione dei dettagli di uno chassis gestito e Gestione dei rack nella documentazione online di XClarity Administrator).

- PUT /canisters/*<UUID>*
- PUT /chassis/*<UUID>*
- PUT /nodes/*<UUID>*